AVAYA

Administering Avaya one-X® Client Enablement Services

Release 6.1 SP3
v1.3
October 2012

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License type(s)

Named User License (NU). End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”). (see “Third-party Components” for more information).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

The open source license text file, `OpenSourceLicense.txt`, is available in the Licenses folder on the Avaya one-X® Client Enablement Services server: `/Licenses/OpenSourceLicense.txt`.

Preventing Toll Fraud

“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll

Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: Administration Overview

Avaya one-X® Client Enablement Services administration overview

The Client Enablement Services Administration application contains the Administration Command Line Client and Administration Web Client application. This application is for the following audience:

- Administrative users
- Auditor users

From the administrative interface, administrative users can configure users, services, and system tasks on Client Enablement Services. They can add and configure the security groups for users of Client Enablement Services during the installation and implementation process. You cannot modify the security groups after the installation.

Administrative users

These users can configure the users, servers, and system functions on Client Enablement Services. Administrative users use the administration application to perform all administrative tasks.

Auditor users

These users have read-only privileges and restricted access to the functions in the Administration application. These users can review Client Enablement Services but cannot make changes to the Client Enablement Services. The *Scheduler* and *Monitor* functions are not available to an *Auditor* user. Other functions return an error if the *Auditor* tries to make a change.

Administration Web Client overview

The Avaya one-X® Client Enablement Services administration application is a Web based application and thus you have the advantage of administering a Client Enablement Services server from any computer. Using this application, you can do the following:

- configure the various servers, which are required for different functionalities, on the Client Enablement Services server
- define system and group profiles

- create users and assign resources to a user
- schedule and administer synchronization, statistics cleanup, database backup
- system administration such as Enterprise Directory, License server, Mobile application, SMS domain, Notification, SNMP traps, SNMP destinations, logging, JDBC connector
- monitor, suspend, and restart various services of Client Enablement Services

The above list of tasks is not a comprehensive list of all tasks that you can do using the administration application. This is just a representative list.

Administration Command Line Client overview

You can also use the Administration Command Line Client as an alternative to the Web based administration application for performing some administering tasks. You can use the Administration Command Line Client when the administration Web client is unavailable due to some issue with the server. Administration Command Line Client is also useful when you must perform bulk operations such as importing users, exporting users.

The command line application, Administration Command Line Client, runs commands for various administrative tasks.

Checklist of administration tasks in the administration application

This checklist lists the important tasks that you must perform in the administration application before users can use the features of the client applications. Note that the order of tasks in this checklist is just a suggestive order.

In order	Configuration	What you should do?	Default value
1	Enterprise directory synchronization	Perform an enterprise directory synchronization to get all users from the LDAP to the unprovisioned users list in Client Enablement Services.	None
2	Dial plan	Create dial plan rules.	None
3	Auxiliary server	Add Session Manager as an auxiliary server.	None
4	Telephony server	Add Communication Manager as the telephony server.	None

In order	Configuration	What you should do?	Default value
5	Messaging server	Add Modular Messaging or Messaging or Communication Manager Messaging as the messaging server.	None
6	Conferencing server	Add Avaya Aura®Conferencing as the conferencing server.	None
7	Presence server	Add Presence Services as the presence server.	None
8	Handset	Add details of the handset server.	Values must be same as mentioned at the time of Client Enablement Services installation.
9	Audio transcoding	Add details of the audio transcoding server.	Values must be same as mentioned at the time of Client Enablement Services installation.
10	System management	Configure the system management features such as upload mobile applications, notification settings, license server details, enterprise directory settings.	None
11	System profile	Leave the system profile settings to default unless required.	Use default values
12	Group profile	Create a new group profile for the user.	None
13	Prototype user	Create one or more prototype users.	None
14	User provisioning	Provision the unprovisioned users.	None
15	Scheduler tasks	Schedule various cleanup and synchronization tasks such as database backup, contact log cleanup, statistics cleanup, enterprise directory synchronization, voice messaging synchronization.	None

In order	Configuration	What you should do?	Default value
16	Monitor tasks	Monitor the server and adapter status. Stop and start the service as required.	none

Chapter 2: Logging in

Logging in to the Avaya one-X® Client Enablement Services Administration application

Procedure

1. In your Web browser, type the Web page address of the Client Enablement Services administration application.

   The default Web page address is `https://<oneXCES_machine>/admin`, where *oneXCES_machine* is the IP address or the Fully Qualified Domain Name (FQDN) of the server that hosts Client Enablement Services.

   HTTP access is disabled by default for security reasons. You must use HTTPS to access the Web page of the administration application.

   For example, if the name of the server that hosts Client Enablement Services is *oneXCES* and the domain is *xyzcorp.com*, the Web page address of your Administration application is `https://oneXCES.xyzcorp.com/admin/`.

   ✱ **Note:**

   When you use a third party reverse proxy with the Client Enablement Services server, you must enable the URL filtering on the reverse proxy to disable access to the administration application from outside the corporate network.

2. In the Logon window, type your administrator **Login ID** and **Password**.

   ✱ **Note:**

   Administrator login ID must be a member of the Client Enablement Services admin security group.

3. Click **Logon**.

Logging in to the Avaya one-X® Client Enablement Services server using SSH

About this task

You can open an SSH session to the Client Enablement Services server. You can either use the user name `root` and password *root01* or the user name `craft` and password *craft01* to log in to the system. These are default passwords, and you can change them.

Craft is a general user; therefore, you must use the root login to perform system administration tasks.

To change the password of the user name root, perform the following tasks:

Procedure

1. Log in to the Client Enablement Services server as `craft/craft01` and then switch the user to root using the command **`su - root`** and password *root01*.
2. In the command prompt, type the command **`passwd`**.
   The system displays the message: `Changing password for the user root`.
3. Enter the new password in the **New UNIX password** field.
4. Re-type the password in the **Retype new UNIX password** field.
   The system displays a message: `all authentication tokens updated successfully`.

   Note:

   Once you change the default password for the root user, use this password for subsequent tasks where you use the root login.

Password security

You cannot administer your password using Avaya one-X® Client Enablement Services administration application. Use the enterprise directory to administer your password. Follow these rules to ensure the security of your system:

- When you create a new password, choose a password that is easy for you to remember but difficult for anyone else to guess.
- Follow the password rules of your organization, such as the length of the password and the number and type of characters in the password, if applicable.
- Ask your supervisor if you need help to create your password.
- Never write down your password.
- Never share your password with anyone.
- Contact your supervisor immediately if you suspect any security problems, such as a computer virus, unusually slow response time, or other abnormal behavior of the system.

Logging out of Avaya one-X® Client Enablement Services

Procedure

1. On the title bar of the Client Enablement Services administration application, click **Logoff**.
2. When the system prompts for confirmation, click **OK**.

Related topics:

Logging in to the Avaya one-X Client Enablement Services Administration application on page 17

Chapter 3: Server administration

Checklist for the Avaya one-X® Client Enablement Services client applications

If you are installing either Avaya one-X® Communicator, or Avaya one-X® Mobile, or both, configure the following servers in the Client Enablement Services administration application:

Servers	Only Avaya one-X® Mobile	Only Avaya one-X® Communicator	Both client applications
Avaya Aura® Communication Manager	Yes	Yes	Yes
Avaya Aura® Session Manager	Yes	Yes*	Yes
Modular Messaging	Yes	Yes	Yes
Avaya Aura® Conferencing	No	Yes	Yes
Avaya Aura® Presence Services	Yes	No	Yes
Audio Transcoding	Yes	No	Yes
Handset Server	Yes	No	Yes
HTTP Server	Yes	No	Yes
WebLM Server	Yes	Yes	Yes
LDAP Server	Yes	Yes	Yes

Legends used in the table:

- Yes - configuration is required
- Yes* - this configuration is optional. If you have an Avaya Aura® setup, then you must configure Session Manager.

Session Manager is required only if you deploy the Avaya Aura® Architecture. If Session Manager is not configured, then the SIP adapter connects directly to Communication Manager.

- No - configuration is not required

Dial Plan

Dial Plan services

Most enterprise directory systems, including Active Directory, store telephone numbers in the standard E.164 format, for example, +19788081234. The E.164 format provides a unique description for each telephone number. Avaya one-X® Client Enablement Services uses a Dial Plan to:

- Convert telephone numbers from the E.164 standard format to a sequence of numbers that the switch can dial or use for Mobile number or Ring also number transformation.
- Convert a sequence of numbers received from the switch to the standard E.164 format.

Note:

Although most enterprise directories store telephone numbers in the E.164 format, this format is not mandatory for dial plan conversions using Client Enablement Services.

Client Enablement Services supports Extension to cellular feature of Communication Manager. The rules for conversion of the dialed string to Extension to cellular number are defined in a separate number transformation table on the Dial Plan page. The Extension to cellular number transformation, therefore, happens independently according to the type of transformation selected, such as Simple, Pattern Matching, or Regular Expression and can be configured to fit the enhanced Extension to cellular feature number format.

In Client Enablement Services, you can configure the number of a user to simultaneously ring a mobile number and other phone numbers when a call arrives in the user's station. When this functionality is set for a user, Communication Manager expects the number format to be in the External Number Dialing Format. You can administer dial plans to configure this number transformation.

Client Enablement Services includes the following Dial Plan transformations:

- Simple Dial Plan transformation
- Pattern Matching transformation
- Regular Expression transformation

Related topics:

Prerequisites on page 23
Adding Dial Plans on page 36
Listing Dial Plans on page 38
Modifying Dial Plans on page 38
Deleting Dial Plans on page 40
Servers field descriptions on page 69

Prerequisites

Expertise

You must work with a subject matter expert who understands how the Dial Plan is configured in the switch to configure a Dial Plan in Avaya one-X® Client Enablement Services. If the Dial Plan configuration in both the switch and Client Enablement Services do not match, telephone calls do not reach the correct recipients.

Client Enablement Services configuration

Each Dial Plan must have a Simple Dial Plan transformation.

If the Dial Plan in the switch includes more complex transformation rules, you can add either a Pattern Matching transformation or a Regular Expression transformation or both. In this case, the Pattern Matching transformation or the Regular Expression transformation takes precedence over the simple dial plan rule.

A Dial Plan has three conversion rules tables: **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to displayed string in Client**, and **Conversion from dialed string to Extension to Cellular number**. You can use either the Pattern Matching transformation or the Regular Expression transformation for each conversion table in the Dial Plan.

Simple Dial Plan transformation

All Dial Plans configured in Avaya one-X® Client Enablement Services must use the Simple Dial Plan transformation. This transformation uses the same number transformation that people use when they automatically convert a telephone number before they begin dialing the number in the switch. For example, in the United States, many users dial 9 before a phone number to make the connection. To call +1(978) 555-1111, they dial 919785551111. A Simple Dial Plan transformation performs the same type of conversion.

The Simple Dial Plan transformation can transform any input into a valid final output. Therefore, this transformation is always the last transformation applied to any number. If you also configure another transformation and it is unable to convert the input to a valid output, Client Enablement Services uses the Simple Dial Plan transformation rule.

Note:

The Simple Dial Plan transforms any input into a valid final output. However, sometimes the transformed output may be a valid telephone number, but this number connects to an incorrect destination. Simple Dial Plan cannot control the output after transformation, but other dial plan entries can do so. Simple Dial Plan provides a good starting point for the configuration, but over time most of the Dial Plan configurations tend to migrate to other Dial Plans. When this migration happens, you can configure the system to stop using Simple Dial Plan by providing a rule that matches any input as the final rule of the other dial plans.

The Simple Dial Plan transformation procedure

The Simple Dial Plan transformation uses a set of values to deduce if the user wants to make one of the following types of calls. It automatically adjusts the number format to match the sequence of numbers expected by the switch:

- Extension to extension call
- Local call
- National call
- International call

Related topics:

Simple Dial Plan transformation usage on page 24
Example: Simple Dial Plan transformation on page 25

Simple Dial Plan transformation usage

Always configure a Simple Dial Plan transformation for each Dial Plan in the switch.

Use Simple Dial Plan transformation for the following types of Avaya one-X® Client Enablement Services implementation:

- The Dial Plan in the switch does not have any complex rules.
- The deployment is at a small to mid-size corporation inside the United States or any other country.
- The deployment is not required to support inter-switch dialing.

Configure Simple Dial Plan transformation with one of the other transformations for corporations where there is an overlap between the call length of extensions and local phone numbers. In addition, due to variations between dial plans, some countries may not be able to use this transformation alone.

Example: Simple Dial Plan transformation

This example describes how a Simple Dial Plan transformation uses the Dial Plan configuration to ensure that telephone numbers dialed in Avaya one-X® Client Enablement Services reach the correct destination.

Dial Plan configuration

Parameter	Value
Main switch number	15553335000
Outside line access code	9
Local Region Prepend	555
Inter-region prepend	1
International prepend	011
National call length	10
Local call length	7
Extension length	5

This Simple Dial Plan transformation does the following:

1. Uses the main switch number as a template for all other telephone numbers.
2. Modifies the telephone number that is dialed by a user to match the template.

Dial Plan results

The Simple Dial Plan transformation uses this Dial Plan configuration to create the following transformations on telephone numbers dialed by users:

Telephone number dialed by user	Transformed telephone number
+15553335111	35111
+15554440000	94440000
+15087641234	915087641234
+551151856200	9011551151856200

Pattern Matching transformation

The Pattern Matching transformation is very similar to the algorithm used by Communication Manager. The system evaluates the Pattern Matching rules in the order that they are specified in the user interface. The first rule to match the input is used as the transformation rule.

The Pattern Matching transformation matches a pattern based on the following three values:

- String at the beginning of the number
- Minimum length of the string
- Maximum length of the string

After the Dial Plan matches the number, the Pattern Matching transformation deletes the specified number of characters and inserts the configured set of characters.

Note:

A Dial Plan has three conversion rules tables: **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to displayed string in Client**, and **Conversion from dialed string to "Extension to Cellular" number**. You can use either the Pattern Matching transformation or the Regular Expression transformation for each conversion table in the dial plan. However, a dial plan can be a combination of either of them.

Related topics:

Pattern Matching transformation usage on page 26

Example: Pattern Matching transformation on page 27

Pattern Matching transformation usage

When to configure the Pattern Matching transformation

Use the Pattern Matching transformation for the following type of Avaya one-X® Client Enablement Services implementations:

- When the Simple Dial Plan transformation cannot convert all required number formats.
- When the telephone number used to dial out depends upon the length of the number and the first digit in the number.
- If the user needs to dial a specific numerical prefix to make international or cell phone calls.
- When a deployment includes switch networks.

For example, in a deployment that includes switch networks, a user in one location can call an employee at another location without dialing a long distance number. Each location has a dedicated switch, which is networked to the switch at the other location. To call a local extension, the user dials 7 plus a five-digit number. To call an extension at the other location, the user dials 8 plus a five-digit number.

When not to configure the Pattern Matching transformation

In the following situations, use Regular Expression transformation in place of Pattern Matching transformation:

- When the telephone number depends upon specific ranges in the number, such as a country code and a city code.
- If the telephone number used to dial out does not require a specific number for the first digit, but instead the first digit can be one of a range of numbers.
- When the Dial Plan requires a large number of rules to match the possible patterns in the telephone numbers.

Example: Pattern Matching transformation

This example describes how Pattern Matching transformation matches patterns to ensure that telephone numbers dialed in Avaya one-X® Client Enablement Services reach the correct destination.

Patterns to be matched

If the cell entry is <blank>, the pattern can match any possible value for that entry.

Starts with	Minimum length	Maximum length	Delete	Prepend	Description
+1555333	12	12	8	6	Internal extension calls. Dial the extension number.
+1555	12	12	5	9	Local calls
+1	12	12	2	91	Domestic long distance calls
+	12	<blank>	1	9011	International calls
<blank>	1	<blank>	0		Not an E.164 number. Dial as is.

Dial plan results

The Pattern Matching transformation uses these patterns to create the following transformations on telephone numbers dialed by users:

Telephone number dialed by user	Transformed telephone number
+15553335111	65111

Telephone number dialed by user	Transformed telephone number
+15553310000	93310000
+15087641234	915087641234
+551155551234	9011551155551234
915552225555	915552225555

Regular Expression transformation

The Regular Expression transformation is the most flexible transformation but also most difficult to configure.

The Regular Expression transformation uses the syntax defined by Java Regular Expressions. This transformation takes the list of regular expressions and replacement patterns that you define and applies them to the telephone number.

Note:

A Dial Plan has three conversion rules tables: **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to displayed string in Client**, and **Conversion from dialed string to "Extension to Cellular" number**. You can use either the Pattern Matching transformation or the Regular Expression transformation for each conversion table in the dial plan. However, a dial plan can be a combination of either of them.

Related topics:

Regular Expression transformation usage on page 28

Example: Regular Expression transformation on page 29

Regular Expression transformation usage

When to use the Regular Expression transformation

Use the Regular Expression transformation when the other transformations are not flexible enough to transform the telephone numbers. For example, use the Regular Expression transformation for the following type of Avaya one-X® Client Enablement Services implementations:

- When the telephone number depends upon specific ranges in the number, such as a country code and a city code.
- If the telephone number used to dial out does not require a specific number for the first digit, but instead the first digit can be one of a range of numbers.
- When the Dial Plan requires a large number of rules to match the possible patterns in the telephone numbers.

When not to use the Regular Expression transformation

Do not use this transformation in the following scenarios:

- Dial Plan in the switch does not have any complex rules.
- Deployment is not required to support inter-switch dialing.
- When the telephone number used to dial out depends upon the length of the number and the first digit in the number.
- If the user needs to dial a specific numerical prefix to make international or cell phone calls.
- When the Dial Plan does not require a large number of rules to match the possible patterns in the telephone numbers.

Example: Regular Expression transformation

This example describes how a Regular Expression transformation matches patterns and regular expressions to ensure that telephone numbers dialed in Avaya one-X® Client Enablement Services reach the correct destination.

Patterns to be matched

Pattern	Replacement	Explanation
\+1555333(\d{4,4})	6$1	Internal extension calls. Dial the extension number.
\+1555(\d{7,7})	9$1	Local calls
\+1(\d{10,10})	91$1	Domestic long distance calls
\+55(\d{2,2}[89]\d{7,7})	9101045855$1	For making calls to Brazil, for any cell phone number that locally starts with an 8 or 9. These numbers must be prefixed by a special number to go through a cheaper carrier.
\+(\d{10,})	9011$1	Any other international number can go through the normal long distance carrier.
(\d{10,10})	91$1	A 10 digit number in a user contact that does not use the E.164 format.
(\d{4,})	$1	Other numbers can be dialed as entered.

Dial plan results

The Regular Expression transformation uses these patterns to create the following transformations on telephone numbers dialed by users:

Telephone number dialed by user	Transformed telephone number
+15553335111	65111
+15553211234	93211234
+15087641234	915087641234
+551191851234	91010458551191851234
+551155551234	9011551155551234
7204441000	917204441000
919785551234	919785551234

Creating rules for a Dial Plan

About this task

Before you create or configure a Dial Plan in Avaya one-X® Client Enablement Services, you must gather information and determine what you need to support the Dial Plan in the switch.

Procedure

1. Obtain the following information from the switch administrator:
   - For all information required in the Dial Plan worksheet in the Client Enablement Services, see Configuration worksheet for Dial Plan on page 297.
   - A list of number formats used for telephony numbers in the enterprise directory system. These formats are the dialed string expected number inputs for the Dial Plan.
   - A list of the expected number formats that the switch shows or dials. These formats form the network rules for the expected numbers received from the network.
2. Analyze the information that you receive and create the rules for the Dial Plan:
   a. Create a table of the dialed number formats for the expected inputs.
   b. Create a table of the formats for the numbers that you expect Client Enablement Services to receive from the network.
   c. Write the E. 164 rules required to transform the expected inputs into each type of expected output number.
   d. Write the network rules required to transform the expected numbers received from the network into each type of expected output.

   e. List the E. 164 rules in order from the most specific to the most general, and eliminate any duplicate rules.
   f. List the network rules in order from the most specific to the most general, and eliminate any duplicate rules.

3. Create a Simple Dial Plan transformation in the Administration application.
4. Run a set of basic sanity tests that covers each of the rules created in step 2 for calls dialed out with the Dial Plan.
5. If the Dial Plan does not ensure that all calls are delivered to the correct recipients, determine whether you need to create a Pattern Matching transformation or a Regular Expression transformation.
6. If you create a new transformation, run a set of basic sanity tests that covers each of your rules for calls dialed out with the Dial Plan.

Related topics:

Example: Creating rules for a Dial Plan on page 31

Example: Creating rules for a Dial Plan

This example creates the rules for a Pattern Matching transformation.

This example lists the tasks involved in step 2 of Creating rules for a Dial Plan on page 30.

You should look at two aspects when configuring a dial plan:

- transformation of a number received from the switch to a number that can be used for contact lookup
- transformation of a number received from the user, either as a contact lookup or as a number typed as the user's address, to a number that when dialed reaches the user's intended destination.

Transformation of a number from the switch to a contact number

This step requires you to analyze the information that is received from the switch and the information that is configured for contacts, so the phone numbers can be used to represent those contacts.

For this, you need a list of numbers that are sent from the switch, called network numbers, and the numbers as they are stored in the contact list. Numbers in the contact list usually come from the Enterprise Directory, and the recommended practice is that these numbers should be stored in E.164 number format.

Note:

Although most enterprise directories store telephone numbers in the E.164 format, this format is not mandatory for dial plan conversions using Client Enablement Services.

Expected numbers that Avaya one-X® Client Enablement Services receives from the network

The switch displays these numbers on the user extension and in Client Enablement Services. They do not have to be numbers that a user can dial.

Number received from network	Description
75247	Local extension call
23657	Call from number in second location of switch network
5553341234	Call from local number
4447641234	Call from domestic long distance telephone number
551151856280	Call from international telephone number. This number can vary significantly.

Corresponding contact number format

The enterprise directory uses these formats to store telephone numbers.

Expected number input	Description
+15553375247	Local extension
+12228523657	Number in second location of switch network
+15553341234	Local number
5553341234	Personal directory number that is not formatted using the E.164 format
+14447641234	Domestic long distance telephone number
+551151856280	International telephone number

Network rules to transform the numbers received from the network into expected output

After you have the list of numbers expected from the network, write the network rules needed to transform each sequence numbers into the expected output.

In this table, if the cell entry is <*blank*>, the pattern can match any possible value for that entry.

Number from network	Description	Expected Output	Rule
75247	Local extension call	+15553375247	Starts with: 7 Minimum length: 5 Maximum length: 5 Delete: 0 Prepend: +155533
23657	Call from number in	+12228523657	Starts with: 2 Minimum length: 5

Number from network	Description	Expected Output	Rule
	second location of switch network		Maximum length: 5 Delete: 0 Prepend: +122285
5553341234	Call from local number	+15553341234	Starts with: 555 Minimum length: 10 Maximum length: 10 Delete: 0 Prepend: +1
4447641234	Call from domestic long distance telephone number	+14447641234	Starts with: <*blank*> Minimum length: 10 Maximum length: 10 Delete: 0 Prepend: +1
551151856280	Call from international telephone number. This number can vary significantly.	+551151856280	Starts with: <*blank*> Minimum length: 11 Maximum length: 15 Delete: 0 Prepend: +

Organize the network rules and eliminate duplicates

After you have the sequence of network rules, organize the rules in order from the most specific to the most generic. Then, delete any duplicate rules.

In this table, if the cell entry is <*blank*>, the pattern can match any possible value for that entry.

Number from network	Description	Expected Output	Rule	#
75247	Local extension call	+15553375247	Starts with: 7 Minimum length: 5 Maximum length: 5 Delete: 0 Prepend: +155533	1
23657	Call from number in second location of switch network	12228523657	Starts with: 2 Minimum length: 5 Maximum length: 5 Delete: 0 Prepend: +122285	2
	Call from local number			Duplicate rule. Deleted.

Number from network	Description	Expected Output	Rule	#
4447641234	Call from domestic long distance telephone number	+14447641234	Starts with: <*blank*> Minimum length: 10 Maximum length: 10 Delete: 0 Prepend: +1	3
551151856280	Call from international telephone number. This number can vary significantly.	+551151856280	Starts with: <*blank*> Minimum length: 11 Maximum length: 15 Delete: 0 Prepend: +	4

Transformation of a number received from the user to a number that can be dialed by the switch

This step requires you to analyze the number format that is received from the user and transform that number into a number that can be dialed by the switch. The number received from the user can either be a result of a contact lookup, or a result of the user typing the number to be dialed. There is some flexibility on how the user input can be transformed into valid outputs.

E. 164 formats for the expected inputs

The enterprise directory uses these formats to store telephone numbers.

Expected number input	Description
+15553375247	Local extension
+12228523657	Number in second location of switch network
+15553341234	Local number
5553341234	Personal directory number that is not formatted using the E.164 format
+14447641234	Domestic long distance telephone number
+551151856280	International telephone number

E. 164 rules to transform the formats into expected output

After you have the expected E. 164 formats, write the E. 164 rules needed to transform each format into the expected output.

In this table, if the cell entry is <*blank*>, the pattern can match any possible value for that entry.

Expected number input	**Description**	**Expected Output**	**Rule**
+15553375247	Local extension	75247	Starts with: +1555337 Minimum length: 12 Maximum length: 12 Delete length: 7
+12228523657	Number in second location of switch network	23657	Starts with: +1222852 Minimum length: 12 Maximum length: 12 Delete length: 7
+15553341234	Local number	915553341234	Starts with: +1555 Minimum length: 12 Maximum length: 12 Delete length: 1 Prepend: 9
5553341234	Personal active directory number that is not formatted using the E.164 format	915553341234	Starts with: <*blank*> Minimum length: 10 Maximum length: 10 Delete length: 0 Prepend: 91
+14447641234	Domestic long distance telephone number	914447641234	Starts with: +1 Minimum length: 12 Maximum length: 12 Delete length: 1 Prepend: 9
+551151856280	International telephone number	9011551151856280	Starts with: + Minimum length: 10 Maximum length: 15 Delete length: 1 Prepend: 9011

Organize the E. 164 rules and eliminate duplicates

After you have the sequence of E. 164 rules, organize the rules in order from the most specific to the most generic. The most specific rules match the most digits in the number. The most generic rules match the least digits. For example, the Pattern Matching transformation must first attempt to match the number to a more specific rule for numbers that start with +1555. If that match fails, then the transformation must next attempt to match the number to a more generic rule for numbers that start with +1.

Delete all duplicate rules from the table.

In this table, if the cell entry is <*blank*>, the pattern can match any possible value for that entry.

Expected number input	Description	Expected Output	Rule	#
+15553375247	Local extension	75247	Starts with: +1555337 Minimum length: 12 Maximum length: 12 Delete length: 7	1
+12228523657	Number in second location of switch network	23657	Starts with: +1222852 Minimum length: 12 Maximum length: 12 Delete length: 7	2
	Local number			Duplicate rule. Deleted.
5553341234	Personal active directory number that is not formatted using the E.164 format	915553341234	Starts with: <*blank*> Minimum length: 10 Maximum length: 10 Delete length: 0 Prepend: 91	3
+14447641234	Domestic long distance telephone number	914447641234	Starts with: +1 Minimum length: 12 Maximum length: 12 Delete length: 1 Prepend: 9	4
+551151856280	International telephone number	0911551151856280	Starts with: + Minimum length: 10 Maximum length: 15 Delete length: 1 Prepend: 9011	5

Adding Dial Plans

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Dial Plan**.
3. On the Dial Plans page, click **Add New Dial Plan**.

   If you want to add Pattern Match and Regular Expression rules to the Dial Plan, modify the Dial Plan using the steps in Modifying Dial Plans on page 38 after you complete these steps.

4. On the Add New Dial Plan page, enter the appropriate information and click **OK** to add the **Dial Plan**.

   For more information on the fields, see Dial Plan field descriptions on page 81.

5. In the **Dial Plan Transformation** section of the page, you can transform a phone number to display the **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to Displayed string in Client**, and **Conversion from configured string to PBX (Extension to Cellular Feature)** numbers from this dial plan to determine if the Dial Plan is correctly configured.

   - **Conversion from dialed string to PBX dialable string**. Displays how the dial plan converts the number entered by the user, either by typing the number or selecting the number from the contact information, to a string that Communication Manager can use to dial the destination.
   - **Conversion from ANI to Displayed string in Client**. Displays how the dial plan converts an ANI to display on the client application. This is used to display the ANI in an E.164 format or a format that matches with the numbers configured on the LDAP, so that a user can search for a contact in the client application.
   - **Conversion from configured string to PBX (Extension to Cellular Feature)**. Displays how the dial plan converts a mobile or also ring number to a string for Mobility.

     This transformation rule is used to convert the mobile number the user enters on their mobile device as per the rules defined in the ARS table configured on the Communication Manager.

   a. In the **Number to Transform** field, enter the phone number.

   b. Click **Transform** to display the **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to Displayed string in Client**, and **Conversion from configured string to PBX (Extension to Cellular Feature)** numbers for that number in the dial plan.

6. Click **Test** to run a short test of your entries.
   The system displays the test results immediately so you can make any necessary changes.

7. Click **Reset** to restore the settings to the last saved page or the default values if this is a new object.

8. Click **Cancel** to exit the page without making any changes.

Related topics:

Dial Plan services on page 22

Servers field descriptions on page 69

Listing Dial Plans

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Dial Plan**.
3. On the Dial Plans page, click the name of a Dial Plan in the **Handle** field to display the Modify Dial Plan page.

Related topics:

Dial Plan services on page 22

Servers field descriptions on page 69

Modifying Dial Plans

About this task

Select a Dial Plan to modify its settings.

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Dial Plan**.
3. From the list of the Dial Plans configured on the system, click the name of a Dial Plan in the **Handle** field to display the Modify Dial Plan page.
4. Modify the **Dial Plan**. See Dial Plan field descriptions on page 81.
5. Add Conversion Rules.

   The **Conversion Rules** table is divided into 3 sections: **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to displayed string in Client**, and **Conversion from configured string to PBX (Extension to Cellular Feature)**. Select the desired algorithm **Pattern Match** or **Regular Expression** for each conversion rule.
6. For the **Pattern Match** algorithm, complete the following fields:

   a. Select **Add** to add the new conversion rule to the **Dial Plan**.

   b. In **Sort Position**, enter the order in which this rule is executed from the list of rules in this section. Enter 1 for first, 2 for second, and so on. When you save the dial plan, the order is displayed in increments of 5, 1 becomes 5, 2 becomes 10, and so on.

c. In **Minimum Length**, enter the minimum number of digits allowed in the phone number.

d. In **Maximum Length**, enter the maximum number of digits allowed in the phone number.

e. In **Starts With**, enter the pattern of the algorithm to match the **Regional Prefix**. For example, if the value of **Regional Prefix** is 978, enter +1978.

f. In **Delete Length**, enter the number of digits to delete from the beginning of the phone number.

g. In **Prepend**, enter the numbers you want to append to the beginning of the phone number.

7. For the **Regular Expression** algorithm, complete the following fields:

   a. Select **Add**, to add the new conversion rule to the **Dial Plan**.

   b. In **Sort Position**, enter the order in which this rule is executed from the list of rules in this section. Enter 1 for first, 2 for second, and so on. When you save the dial plan, the order is displayed in increments of 5, 1 becomes 5, 2 becomes 10, and so on.

   c. In **Regular Expression**, enter the Regular Expression pattern that applies to the phone number.

   d. In **Prepend**, enter the replacement pattern that applies to the phone number. A Regular Expression pattern of \+14259(\d{7.}) and a Replacement pattern of 9$1 could transform the phone number +14252417293 to 92417293.

8. To delete one or more conversion rule from the Existing Rules, select the **Del** check box adjacent to a rule, and click **Save**.

9. In the **Dial Plan Transformation** section of the page, you can transform a phone number to display its **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to displayed string in Client**, and **Conversion from configured string to PBX (Extension to Cellular Feature)** numbers from this dial plan to determine if these changes are correctly configured.

   - **Conversion from dialed string to PBX dialable string**. Displays how the dial plan converts the number entered by the user, either by typing the number or selecting the number from the contact information, to a string that Communication Manager can use to dial the destination.

   - **Conversion from ANI to Displayed string in Client**. Displays how the dial plan converts an ANI to display on the client application. This is used to display the ANI in an E.164 format or a format that matches with the numbers configured on the LDAP, so that a user can search for a contact in the client application.

   - **Conversion from configured string to PBX (Extension to Cellular Feature)**. Displays how the dial plan converts a mobile or also ring number to a string for Mobility.

This transformation rule is used to convert the mobile number the user enters on their mobile device as per the rules defined in the ARS table configured on the Communication Manager.

a. In the **Number to Transform** field, enter the phone number.
b. Click **Transform** to display the **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to Displayed string in Client**, and **Conversion from configured string to PBX (Extension to Cellular Feature)** numbers for that number in the dial plan number.

10. Click **Test** to run a short test of your changes. The results of the test are displayed immediately so you can make any necessary changes.
11. Click **Save** to update the **Dial Plan**.

    ✱ **Note:**

    Use the Synchronize feature to synchronize the mobile numbers on Communication Manager after you change the dial plan or call routing configuration on Client Enablement Services. See Synchronize feature on page 48.
12. Click **Reset** to restore the settings to the last saved page or the default values if this is a new object.
13. Click **Delete** to delete the dial plan.
14. Click **Cancel** to exit the page without making any changes.

Related topics:

Dial Plan services on page 22

Servers field descriptions on page 69

Deleting Dial Plans

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Dial Plan**.

   The Dial Plans page displays a list of the Dial Plans configured on the system.
3. Click the name of a Dial Plan in the **Handle** field to display the Modify Dial Plan page for the Dial Plan.
4. Click **Delete** to delete the Dial Plan from Avaya one-X® Client Enablement Services.
5. Click **Yes** at the prompt to complete the deletion.

Client Enablement Services displays a successful deletion message.

Result

When you delete a Dial Plan, and if the deleted Dial Plan is associated to any Telephony, Voice Messaging, or Conferencing servers, then these servers no longer have this Dial Plan.

Related topics:

Dial Plan services on page 22

Servers field descriptions on page 69

Telephony servers and Auxiliary servers

The telephony server adapter for Communication Manager service on Avaya one-X® Client Enablement Services provide computer telephony integration (CTI) with Communication Manager switches to provide a single Avaya interface to the portfolio of Avaya products.

Client Enablement Services uses the telephony adapter to extend calls to employees' mobile phones through Communication Manager. This supports following functionalities:

- Manages call routing of corporate PBX extensions directly to other locations, such as a mobile phone.
- Routes incoming calls based on the identity of an individual caller by using call routing rules, also known as block all calls. For example, employees can receive calls from their manager, but all other incoming calls are redirected to the voice mail.
- Calls a destination using a callback device, such as the mobile phone or another phone.
- Enables call logging.

Auxiliary servers act as a supplementary server to the Telephony servers. Add Session Manager as an auxiliary server. Session Manager acts as a link between Communication Manager and Client Enablement Services in the Avaya Aura environment. This link can be established either over TCP or TLS. To establish a link over TLS, you must integrate System Manager with Client Enablement Services at the time of installation.

When the link fails between Client Enablement Services and Session Manager, Client Enablement Services establishes a direct link with Communication Manager. This direct link can be established over either TCP or TLS.

Client Enablement Services can integrate with maximum four Session Managers at a time.

This section describes how to configure **Telephony** servers and **Auxiliary Servers**, and the steps to enable them to communicate with each other.

Related topics:

[SIP Local](#) on page 145

Adding Auxiliary servers

Before you begin

For TLS connectivity between Communication Manager and the Avaya one-X® Client Enablement Services server through Avaya Aura® Session Manager, you must ensure that the Session Manager you add as an Auxiliary server must be associated with the same System Manager that was configured in the Client Enablement Services server at the time of Client Enablement Services installation.

If the Session Manager you are configuring is not associated with the same System Manager, the Session Manager does not trust the certificate of the Client Enablement Services server and the TLS connection fails.

> ✱ **Note:**
>
> TLS connectivity among Client Enablement Services, Session Manager, and Communication Manager requires TLS all the way through. Therefore, Session Manager must have a TLS link to Communication Manager and to Client Enablement Services.

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Auxiliary Servers**.
3. On the Auxiliary Servers page, in the **Server Type** drop-down list, select the version of Session Manager installed on your system.
4. Click **Add**.
5. On the Add Auxiliary Server Configuration page, enter the server configuration information and click **Save** to add the server.

   For more information, see [Auxiliary server (Session Manager) field descriptions](#) on page 73.
6. Click **Test** to run a short test of your entries. The results of the test are displayed immediately so you can make any necessary changes.
7. Click **OK** to add the auxiliary server.
8. Click **Reset** to restore the settings to the last saved page.
9. Click **Cancel** to exit the page without making any changes.

Listing Auxiliary servers

Procedure

1. Select the **Server** tab.
2. From the left pane, select **Auxiliary Servers**.
3. On the Auxiliary Servers page, click the name of a Session Manager in the **Handle** column.
   The system displays the View Auxiliary Server page for the server.

Related topics:

Servers field descriptions on page 69

Modifying Auxiliary servers

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Auxiliary Servers**.
3. On the Auxiliary Servers page, click the name of a Session Manager in the **Handle** field to modify its settings.
   The system displays the View Auxiliary Server page for the server.
4. Enter the appropriate information and click **Save** to update the server.

   For more information on Session Manager field descriptions, see Auxiliary server (Session Manager) field descriptions on page 73.
5. If you change the IP address of the Session Manager, restart the Telephony service.

   For instructions, see Monitoring Telephony services on page 186.
6. Click **Test** to run a short test of your changes.
   The results of the test are displayed immediately so you can make any necessary changes.
7. Click **Reset** to restore the settings to the last saved page or to restore the default values, if this is a new object.
8. Click **Cancel** to exit the page without making any changes.

Related topics:

Servers field descriptions on page 69

Deleting Auxiliary servers

Before you begin

You must disable the Session Manager before you delete the auxiliary server. Clear the **Enabled** check box on the View Auxiliary Server page to disable the server.

Procedure

1. Select the **Monitors** tab.
2. From the left pane, select **Telephony** to display the status of the Telephony servers and the configured Session Manager.
3. Click **Suspend** in the box that contains the Handle of the Session Manager you want to delete.
4. Select the **Servers** tab.
5. From the left pane, select **Telephony**.
6. On the Telephony Servers page, click the link in the **Handle** column of a telephony server to modify the telephony server.
7. On the View Telephony Server page, in the **Session Manager Selected** field, click the name of the Session Manager you want to delete.
8. Click **Remove** to end the association between the Session Manager and the Communication Manager.
9. Click **Save**.

   Repeat step 6 to 9 for each Telephony server that is associated with the Session Manager you want to delete.
10. From the left pane, select **Auxiliary Servers**.
11. On the Auxiliary Servers page, in the **Handle** column, click the name of the Session Manager you want to delete.
12. On the View Auxiliary Server page, click **Delete** to delete the server from Avaya one-X® Client Enablement Services.
13. Click **Yes** at the prompt to complete the deletion.
    Client Enablement Services displays a successful deletion message.

Adding Telephony servers

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Telephony**.
3. On the Telephony Servers page, in the **Server Type** field, select the version of the Communication Manager installed on your system.
4. Click **Add** to display the Add Telephony Server Configuration page.
5. Enter the appropriate information.

   For more information on the fields, see Telephony server field descriptions on page 69.
6. Add the Session Manager to be used by the Telephony server. Perform the following steps:
   a. In the **Session Manager Available** field, select the name of the Session Manager to add to the Telephony server configuration.
   b. Click **Add** to move the selected server(s) to the **Session Manager Selected** field. You can also click **Add ALL** to move all of the servers.
   c. Repeat these steps to add additional Session Managers to set up a failover strategy. If the first Session Manager on the list fails, the Telephony server uses the next server on the list.
   d. Select the server name and click **Move Up** or **Move Down** to reorder the list.
   e. Select the server name and click **Remove** to remove the server and move it back to the **Session Manager Available** list. You can also select multiple servers and click **Remove All**.
7. Select a dial plan from the **Dial Plan** drop-down list.
8. Add one or more call routing configuration, if required.
   - **Location**
   - **GSM Gateway**
   - **Mobile/Ring also Location**

   For more information, see Adding routing configuration on page 51.
9. Click **OK** to add the server.
10. Click **Test** to run a short test of your entries. The results of the test are displayed immediately so you can make any necessary changes.

    If the test is successful, the View Telephony Server page displays the following message:

    ```
    Test Server Results
    ```

```
INFO: CM <IP address of the Communication Manager> accepting
SIP messages from server <IP address of the Client Enablement
Services server>.
```

Related topics:
Servers field descriptions on page 69

Listing Telephony servers

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Telephony**.
3. On the Telephony Servers page, you can see the list of telephony servers available on your system.
4. Click the name of a Telephony server in the **Handle** column to display the View Telephony Server page for the server.

Related topics:
Servers field descriptions on page 69

Modifying Telephony servers

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Telephony**.
3. On the Telephony Servers page, select a Telephony server in the **Handle** column. The system displays the View Telephony Server page for the server.
4. Enter the server configuration information.

   For more information on the fields, see Telephony server field descriptions on page 69.
5. To make changes to the Session Manager, perform the following steps:
   a. In the **Session Manager Available** field, select the name of the Session Manager to add to the Telephony server configuration.
   b. To move the selected servers to the **Session Manager Selected** field, click **Add**. To move two or more servers, select the servers and click **Add ALL**.

c. To set up a failover strategy, repeat these steps and add additional Session Manager servers.
   If the first Session Manager on the list fails, the Telephony server uses the next server on the list.

d. Select the server name and click **Move Up** or **Move Down** to reorder the list.

e. Select the server name and click **Remove** to remove the server and move it back to the **Session Manager Available**. You can also select multiple servers and click **Remove All**.

6. Select a dial plan from the **Dial Plan** drop-down list.
7. Modify one or more call routing configuration, if required.
   - **Location**
   - **GSM Gateway**
   - **Mobile/Ring also Location**

   For more information, see Modifying routing configuration on page 52.
8. Click **Save** to update the server.

   Restart the server to save your changes.

   Note:

   For more information, see Monitoring Telephony services on page 186.
9. Click **Test** to run a short test of your changes. The results of the test are displayed immediately so you can make any necessary changes.

   If the test is successful, the View Telephony Server page displays the following message:

   ```
   Test Server Results
   ```

   ```
   INFO: CM <IP address of the Communication Manager> accepting
   SIP messages from server <IP address of the Client Enablement
   Services server>.
   ```
10. Click **Reset** to restore the settings to the last saved page or to restore the default values, if this is a new object.
11. Click **Cancel** to exit the page without making any changes.

Related topics:

Servers field descriptions on page 69

Deleting Telephony servers

Before you begin

Before deleting a Telephony server:

- You must disable the Telephony server. Clear the **Enabled** check box on the View Telephony Server page to disable the server.
- You must delete all telephony and mobile telephony resources of all users associated with the server. For more information, see Modifying provisioned users on page 106.

Procedure

1. Click the **Monitors** tab.
2. Click **Suspend** in the box that contains the Handle of the Telephony server you want to delete.
3. Select the **Servers** tab.
4. From the left pane, select **Telephony**.
5. On the Telephony Servers page, in the **Handle** field, click the name of the Telephony server you want to delete.
6. Click **Delete** to delete the Telephony server from Client Enablement Services.
7. Click **Yes** at the prompt to complete the deletion.
   Client Enablement Services displays a successful deletion message.

Related topics:

Servers field descriptions on page 69

Synchronize feature

Synchronize feature synchronizes the Dial Plan and routing configuration changes with the mobile number information stored on Communication Manager.

When you change the Dial Plan or routing configuration in Avaya one-X® Client Enablement Services, the mobile phone numbers associated with the station change. Therefore, to synchronize the information on Client Enablement Services and Communication Manager, you should do a synchronization.

Global changes to phone numbers do not get pushed directly to Communication Manager. Since there is no mechanism to report issues after those changes, you can use the **Synchronize** button to apply the global changes. You can also get report about the issues associated with the changes.

Note:

When you click **Synchronize**, the system displays a warning: `The system will now try to synchronize mobile number information with Communication Manager. Pending changes may be due to dial plan changes, or routing configuration changes. Not all changes may be accepted by CM, so please verify and adjust as needed. Are you sure you want to continue?` Click **OK** if you want to perform the synchronization.

Related topics:

Telephony servers and Auxiliary servers on page 41
Synchronizing dial plan changes on page 49
Call routing on page 49

Synchronizing dial plan changes

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Telephony**.
3. On the Telephony Servers page, select a Telephony server in the **Handle** column.
   The system displays the View Telephony Server page for the server.
4. Click **Synchronize** to synchronize the Dial Plan and routing configuration changes with the mobile number information stored on Communication Manager.

Call routing

Using Call Routing, you can customize how to process a dialed number for a user. Each Call Routing configuration is associated with a Communication Manager configured on the Avaya one-X® Client Enablement Services server, but each Communication Manager can be associated with multiple routing configurations. You can configure the telephony and mobile telephony resource of a user to use these routing configurations.

There are four different contexts where the Client Enablement Services server can send phone numbers to Communication Manager.

- The phone number of the call destination.
- The phone number of a Mobile associated with the extension. This number has origination and termination mapping.

- The phone number of any number other than the Mobile number. This number is also called Ring also number.
- The phone number used for callbacks.

The Client Enablement Services server processes each telephone numbers differently for each context. You can specify a rule for each telephony and mobile telephony resource for each context. You can specify one rule for more than one context on the telephony resource or mobile resource configuration page.

The phone number manipulation for a resource in a specific context enables the implementation of several features like location-based number formatting, GSM gateway configuration (dialing a prefix before dialing the mobile number), and specialized Dial Plans for users who have their personal numbers in a non-standard format.

Each routing configuration is associated with a set of one or more contexts.

Routing configuration type	Database rule	Valid context
GSM Gateway	${prefix}${ops} where “ops” is the result of the dial plan transformation for Extension to cellular numbers.	Mobile number, Callback number
Location	${dialable} where dialable is the result of the transformation of the input using the “PBX dialable string” transformation from the dial plan.	Destination number
Mobile/Ring also Location	${ops} where “ops” is the result of the dial plan transformation for Extension to cellular numbers.	Mobile number, Callback number, and Ring also number

Note:

You cannot modify the database rules.

You can configure several parameters for a Call Routing configuration:

- The Dial Plan used to process the incoming number.
- The Location ID to be used when communicating with Communication Manager.

  Note:

  The Location ID corresponds to the location numbers specified on a Communication Manager. To get a list of locations on a Communication Manager, use the command **`display locations`**.

  - For Destination Routing, the routing configured in the Communication Manager resource or Desk phone resource, this Location ID corresponds to the Communication Manager station location.
  - For the Mobile Resource (SipCM resource), each routing type such as Mobile Routing, Ring-also Routing, and Callback routing can have its own location.
- The prefix to be used when dialing the number.
- Name of the routing configuration.
- The routing configuration that a telephony or mobile telephony resource uses.

For example, the prefix and the dial plan you configure for a GSM Gateway routing configuration are used when setting the user’s mobile phone on Communication Manager. It is expected that, when configuring mobile phones to use GSM gateways, the switch administrator configures a prefix to route the call to the GSM gateway. On the other hand, in Location routing configuration, you can configure only the dial plan used to transform the user input into a number that is dialable by the Communication Manager.

Note:

When the user makes a callback call using the desk phone as the originating entity, then for:

- H.323. The desk phone directly calls the destination number.
- SIP. User needs to first pick up the desk phone receiver, and only then the destination number is called.

Related topics:

Telephony servers and Auxiliary servers on page 41
Synchronize feature on page 48
Adding routing configuration on page 51
Modifying routing configuration on page 52
Deleting routing configuration on page 53

Adding routing configuration

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Telephony**.
3. On the Telephony Servers page, click the name of a Telephony server in the **Handle** field to display the View Telephony Server page for the server.
4. Perform one of the following:
   - Click **Add** in the **Location** section to add a routing configuration for a destination number.

- Click **Add** in the **GSM Gateway** section to add a routing configuration for a mobile number or a callback number.
- Click **Add** in the **Mobile / Ring also Location** section to add a routing configuration for a mobile number, or a callback number, or a ring also number.

5. On the Add Routing Configuration page, enter the appropriate information.

   For more information on the fields, see Routing Configuration field descriptions on page 85.
6. Click **OK** to add the destination routing configuration.
7. Click **Reset** to restore the settings to the last saved page or, if this is a new object to the default values.
8. Click **Cancel** to exit the page without making any changes.

Modifying routing configuration

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Telephony**.
3. On the Telephony Servers page, click the name of a Telephony server in the **Handle** field to display the View Telephony Server page for the server.
4. Click the **Name** link of the routing configuration you want to modify.
5. On the View Routing Configuration page, enter the appropriate information.

   For more information on the fields, see Routing Configuration field descriptions on page 85.
6. Click **Save** to save the changes made to the routing configuration.

   Note:

   Use the Synchronize feature to synchronize the mobile numbers on Communication Manager after you change the dial plan or call routing configuration on Client Enablement Services. See Synchronize feature on page 48.
7. Click **Delete** to delete the routing configuration.
8. Click **Reset** to restore the settings to the last saved page.
9. Click **Cancel** to exit the page without making any changes.

Deleting routing configuration

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Telephony**.
3. On the Telephony Servers page, click the name of a Telephony server in the **Handle** field to display the View Telephony Server page for the server.
4. Perform one or more of the following:
   - Click **Delete** in the **Action** column of the **Location** section to delete a routing configuration for a destination number.
   - Click **Delete** in the **Action** column of the **GSM Gateway** section to delete a routing configuration for a mobile number or a callback number.
   - Click **Delete** in the **Action** column of the **Mobile / Ring also Location** section to delete a routing configuration for a mobile number, or a callback number, or a ring also number.

   Note:

   Use the Synchronize feature to synchronize the mobile numbers on Communication Manager after you delete a call routing configuration. See Synchronize feature on page 48.

Voice Messaging servers

Avaya one-X® Client Enablement Services integrates with Modular Messaging servers or Messaging servers or Communication Manager Messaging server for synchronizing the voice messages stored on the mailbox of the users. This integration provides the client applications messaging capabilities such as viewing, hearing, and deleting voice mail messages.

The messaging server communicates with Communication Manager and the Telephony servers to provide these capabilities.

Note:

Client Enablement Services integrates with messaging servers using only the Avaya message store, and not any other e-mail message stores.

Related topics:

Installing the voice messaging server security certificates on page 54
Creating a directory for the Voice Messaging server on page 55
Adding Voice Messaging servers on page 55
Listing Voice Messaging servers on page 56
Modifying Voice Messaging servers on page 57
Deleting Voice Messaging servers on page 58
Servers field descriptions on page 69

Installing the voice messaging server security certificates

About this task

To secure a communication channel between Avaya one-X® Client Enablement Services and the voice messaging server, configure the server certificates to secure the Java mail API. The Java mail API is used to connect the IMAP connection to the voice messaging server. These certificates establish a trust relationship between Client Enablement Services and the voice messaging server.

Install the voice messaging server security certificates as part of the **Voice Messaging** server configuration on the Administration Web Client.

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Voice Messaging**.
   The Voice Messaging page displays a list of the voice messaging server configured on the Client Enablement Services server.
3. Click the name of a voice messaging server in the **Handle** field to display the Modify Voice Messaging Server Configuration page for the server.
4. In the **SSL Certificate** field, click **Retrieve SSL Certificate**.

   For more information on the fields, see Voice Messaging server field descriptions on page 74.
5. Click **Save** to update the server.

   Note:

   You must restart the voice messaging adapter to save your changes. For more information, see Monitoring Voice Messaging services on page 186.
6. Click **Test** to run a short test of your changes.
   The results of the test are displayed immediately so you can make any necessary changes.
7. Click **Reset** to restore the settings to the last saved page or, if this is a new object the default values.

8. Click **Cancel** to exit the page without making any changes.

Creating a directory for the Voice Messaging server

Before you begin

Perform this task after you install Avaya one-X® Client Enablement Services, and before you configure the Voice Messaging server in the administration application.

About this task

The Avaya one-X® Client Enablement Services server runs with the Application server user, which is a not a root user. Therefore, if you do not use the default temp directory for the Voice Messaging server, you must create a directory and provide the Application server user with read/write permissions. The default temp directory that is generated by the system for the Voice Messaging server is `/msgworkdirectory`.

Perform this task only when you configure the server for Voice Messaging in the Administration application, and you do not plan to use the default temp directory. Follow the below steps to create a new directory.

Procedure

1. Determine the name for the Voice Messaging server directory: *Messages Temp Directory*
2. Create the directory.

   You should create the directory in the home directory for the Application server user.

   For example, `/home/appsvr/chicagomsgworkdirectory`.
3. Execute the following command for the directory to give the Application server user read/write privileges: `chown -R` *`appsvr:appsvr / pathtonewmsgworkdirectory`*

   In this command, */pathtonewmsgworkdirectory* is the relative path from the home directory of the Application server user to the directory that you created.

Adding Voice Messaging servers

Procedure

1. Select the **Servers** tab.

2. From the left pane, select **Voice Messaging**.
3. On the Voice Messaging page, in the **Server Type** field, select the version number of the messaging server installed on the system.
4. Click **Add** to display the Add Voice Messaging Server Configuration page.
5. Enter the appropriate information and click **OK** to add the server.

   For more information on the fields, see Voice Messaging server field descriptions on page 74.
6. Click **Test** to run a short test of your entries.
   The system displays the results of the test immediately so you can make the necessary changes.

   Note:

   In Client Enablement Services, the messaging server security certificates are automatically installed when you add a Voice Messaging server. However, if the server test fails, see Installing the voice messaging server security certificates on page 54.
7. Perform a Voice Messaging synchronization after adding a messaging server.

   See Scheduling Voice Messaging Synchronization on page 132.

Related topics:

Voice Messaging servers on page 53
Servers field descriptions on page 69

Listing Voice Messaging servers

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Voice Messaging**.
3. On the Voice Messaging Servers page, click the name of a messaging server in the **Handle** column.
   The system displays the Modify Voice Messaging Server page for the server.

Related topics:

Voice Messaging servers on page 53
Servers field descriptions on page 69

Modifying Voice Messaging servers

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Voice Messaging**.
3. On the Voice Messaging page, click the name of a messaging server in the **Handle** field.
   The system displays the Modify Voice Messaging Server Configuration page for the server.
4. Enter the appropriate information and click **Save** to update the server.

   For more information on the fields, see Voice Messaging server field descriptions on page 74.

   > **Note:**
   >
   > You must restart the messaging server adapter to save your changes. For more information, see Monitoring Voice Messaging services on page 186.
5. Click **Test** to run a short test of your changes.
   The results of the test are displayed immediately so you can make any necessary changes.
6. Perform a Voice Messaging synchronization after modifying a messaging server.

   See Scheduling Voice Messaging Synchronization on page 132.
7. Click **Reset** to restore the settings to the last saved page or, if this is a new object the default values.
8. Click **Cancel** to exit the page without making any changes.

Related topics:

Voice Messaging servers on page 53
Servers field descriptions on page 69

Deleting Voice Messaging servers

Before you begin

Before deleting a **Voice Messaging** server:

- You must disable the **Voice Messaging** server. Clear the **Enabled** check box on the View Voice Messaging Server page to disable the server.
- You must delete all the Voice Messaging resources associated with the voice messaging server. For more information, see Modifying provisioned users on page 106.

Procedure

1. Click the **Monitors** tab.
2. From the left pane, select **Voice Messaging** to display the messaging servers.
3. Click **Suspend** in the box that contains the Handle of the messaging server you want to delete.
4. Select the **Servers** tab.
5. From the left pane, select **Voice Messaging**.
6. On the Voice Messaging Servers page, go to the **Handle** field, and click the name of the messaging server you want to delete.
7. To delete the server from Avaya one-X® Client Enablement Services, click **Delete**.
8. Click **Yes** at the prompt to complete the deletion.
   Client Enablement Services displays a successful deletion message.

   If you have not deleted the voice messaging resource assigned to the user, the system displays an error message.

   ```
   Server <voice messaging server handle> is still referenced by
   users. Please remove it from the users and retry.
   ```

Related topics:

Voice Messaging servers on page 53
Servers field descriptions on page 69

Conferencing services

Conferencing servers with Avaya one-X® Client Enablement Services integration provide bridge conferencing capabilities such as creating on-demand conferences and controlling a live conference to Avaya one-X® Communicator client application.

Bridged conferences are not like conference calls through phone services which is generally limited to 6 parties. Large number of participants can join a bridge conference and one or more moderators control the bridge. Using the client application, some of the tasks the bridge conference moderators can do are:

- add participants
- drop participants
- mute participants
- put the participants line on hold
- secure the conference room by blocking participants from joining the conference

Related topics:

Creating a directory for the Conferencing server on page 59
Adding Conferencing servers on page 60
Listing Conferencing servers on page 61
Modifying Conferencing servers on page 61
Deleting Conferencing servers on page 62
Servers field descriptions on page 69

Creating a directory for the Conferencing server

Before you begin

Perform this task after you install Avaya one-X® Client Enablement Services and before you configure the Conferencing server in the administration application.

About this task

You must create a directory for the Conferencing server, and provide the Application Server user with read/write permissions. There is no default directory for the Conferencing server. Follow the steps below to create a directory for the Conferencing server.

Procedure

1. Determine the name for the Conferencing server directory: `BCAPI Logger Directory`

2. Create the directory in the home directory for the Application server user.
   For example, `/home/appsvr/chicagobcapitmpdirectory`
3. Execute the following command for the directory to give the Application server user read/write privileges: `chown -R` *`appsvr:appsvr /pathtonewbcapitmpdirectory`*

   In this command, */pathtonewbcapitmpdirectory* is the relative path from the home directory of the Application server user to the directory that you created.

Adding Conferencing servers

Procedure

1. Select the **Servers** tab.
2. To display a list of the servers on the system, from the left pane, select **Conferencing**.
3. In the **Server Type** field, select the version number of the Conferencing server installed on the system.
4. Click **Add** to display the Add Conferencing Server Configuration page.
5. Enter the appropriate information and click **OK** to add the server.

   For more information on the fields, see Conferencing server field descriptions on page 78.
6. Click **Test** to run a short test of your entries. The results of the test are displayed immediately so you can make any necessary changes.

   Note:

   If you have entered correct credentials, but the test fails and the system displays an error message that the Meeting Exchange server is not visible and prompts you to verify the ports and the IP address. You can ignore this message, save the Meeting Exchange profile, and then restart the Meeting Exchange adaptor. When you restart the adaptor, the status of the connection changes to **Connected**. You can now run the Meeting Exchange profile test again.
7. Click **Reset** to restore the settings to the last saved page or, if this is a new page, the default values.
8. Click **Cancel** to exit the page without making any changes.

Related topics:

Conferencing services on page 59

Servers field descriptions on page 69

Listing Conferencing servers

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Conferencing**.
   The Conferencing Servers page displays a list of the Conferencing servers installed on the system.
3. Click the name of a Conferencing server in the **Handle** field to display the View Conferencing Server page for the server.

Related topics:

Conferencing services on page 59
Servers field descriptions on page 69

Modifying Conferencing servers

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Conferencing**.
   The Conferencing Servers page displays a list of the Meeting Exchange servers installed on the system.
3. Click the name of a Conferencing server in the **Handle** to display the View Conferencing Server page for the server.
4. Enter the appropriate information and click **Save** to update the server. For more information on the fields, see Conferencing server field descriptions on page 78.

   Note:

   You must restart the conferencing adapter to save your changes. For more information, see Monitoring Conferencing services on page 187.
5. Click **Test** to run a short test of your changes. The results of the test are displayed immediately so you can make any necessary changes.
6. Click **Reset** to restore the settings to the last saved page or, if this is a new object the default values.

7. Click **Cancel** to exit the page without making any changes.

Related topics:

Conferencing services on page 59

Servers field descriptions on page 69

Deleting Conferencing servers

Before you begin

Before deleting a Conferencing server:

- You must disable the Conferencing server. Clear the **Enabled** check box on the View Conferencing Server page to disable the server.
- You must delete all Conferencing resources associated with the server. For more information, see Modifying provisioned users on page 106.

Procedure

1. Click the **Monitors** tab.
2. From the left pane, select **Conferencing** to display the Conferencing servers.
3. Click **Suspend** in the box that contains the Handle of the Conferencing server you want to delete.
4. Select the **Servers** tab.
5. From the left pane, select **Conferencing**.
6. At the Conferencing servers page, go to the **Handle** field and click the name of the Conferencing server you want to delete.
7. Click **Delete** to delete the Conferencing server from Avaya one-X® Client Enablement Services.
8. Click **Yes** at the prompt to complete the deletion.
   Client Enablement Services displays a successful deletion message.

Related topics:

Conferencing services on page 59

Servers field descriptions on page 69

Presence Services server

You can integrate a Presence Services server with Avaya one-X® Client Enablement Services. Presence Services provides presence capabilities to the client applications such as Avaya one-X® Mobile.

- Aggregated presence. Aggregated presence is the combination of presence status such as Available, Busy, Unavailable, Out of Office and system message such as *On a call* or personal message such as *Making quarterly team plan*.
- Channel presence. Channel presence shows the presence status of the user on various channels such as telephone, e-mail, and Microsoft Office Communicator (MOC). The phone state on the client application may show free or busy status. The Instant Messaging (IM) icon on the client application appears either free, busy, or user can set the status to appear as offline.

Note:

Presence feature also provides instant messaging and presence capabilities if Presence Services is integrated with Microsoft Office Communicator (MOC).

Avaya one-X® Communicator connects to the Presence Services server directly. But when you assign a presence resource to an Avaya one-X® Communicator user in the Client Enablement Services administration application , any change in the presence status on one client application is also reflected on the other client application.

The Presence Services server stores and updates presence information for each user on Client Enablement Services. You can configure the presence access level on System Manager. You can manage Access Control Lists and add watchers for a user in System Manager.

Note:

- You can add only one Presence Services server to Client Enablement Services.
- Client Enablement Services does not support integration with the Avaya Presence Services server if you are using Microsoft Active Directory Application Mode (ADAM) as the enterprise directory.

Related topics:

Configuring the Presence Services server for Avaya one-X Client Enablement Services
Adding the Presence server on page 64
Listing the Presence server on page 64
Modifying the Presence server on page 65
Deleting the Presence server on page 65
Servers field descriptions on page 69
Configuring Presence access level on page 280

Adding the Presence server

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Presence**.
3. On the Presence Servers page, in the **Server Type** field, select **PS 6.1**

   PS 6.1 is the version number of the Presence server that you want to configure for presence features.
4. Click **Add** to display the Add Presence Server Configuration page.
5. Enter the appropriate information and click **OK**.

   For more information on the fields, see Presence server field descriptions on page 79.
6. Restart the presence service adapter to ensure that the presence adapter is in connected state.

   For more information on restarting the presence adapter, see Monitoring Presence services on page 188.

Related topics:

Presence Services server on page 63
Servers field descriptions on page 69

Listing the Presence server

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Presence**.
3. The Presence Servers page displays the Presence server that you have configured.

   If you want to view the details of the Presence server, click the handle of the Presence server to display the View Presence Server page for the server.

Related topics:

Presence Services server on page 63
Servers field descriptions on page 69

Modifying the Presence server

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Presence**.
3. On the Presence Server page, click the handle of the Presence server in the **Handle** column.
   The system displays the View Presence Server page.
4. Enter the appropriate information and click **Save** to update the server.

   For more information on the fields, see Presence server field descriptions on page 79.

   Note:

   You must restart the presence service adapter to save your changes. For more information, see Monitoring Presence services on page 188.
5. Click **Reset** to restore the settings to the last saved page or, if this is a new object the default values.
6. Click **Cancel** to exit the page without making any changes.

Related topics:

Presence Services server on page 63
Servers field descriptions on page 69

Deleting the Presence server

Before you begin

Before deleting a Presence server:

- You must disable the Presence server. Clear the **Enabled** check box on the View Presence Server page to disable the server.
- You must delete all Presence resources associated with the server. For more information, see Modifying provisioned users on page 106.

Procedure

1. Click the **Monitors** tab.
2. From the left pane, select **Presence** to display the Presence server.

3. Click **Suspend** in the box that contains the **Handle** of the server.
4. Select the **Servers** tab.
5. From the left pane, select **Presence**.
6. On the Presence Servers page, click the handle of the Presence server in the **Handle** column.
7. Click **Delete** to delete the Presence server from Client Enablement Services.
8. Click **Yes** at the prompt to complete the deletion.
   Client Enablement Services displays a successful deletion message.

Related topics:

Presence Services server on page 63
Servers field descriptions on page 69

Extracting Avaya one-X® Client Enablement Services certificates

About this task

On the Presence Servers screen, the system displays a list of certificates stored in the Client Enablement Services trust store. In the table, **CN** is the certificate name and **Alias** is the alias used, if any.

These certificates are installed during the installation of Client Enablement Services server. You should validate the certificates in the Client Enablement Services server trust store.

You can extract a certificate to either validate the version of the certificates or to have a back up repository for certificates in your local machine. To extract a certificate, perform the following steps:

Procedure

1. In the administration application, select the **Servers** tab.
2. From the left pane, select **Presence**.
3. On the Presence Servers page, click the **Extract** link in the **Extract Certificate** column.
4. In the **File Download** dialog, click **Save** to save the certificate at a location of your choice.

Related topics:

[Avaya one-X Client Enablement Services certificates](#) on page 315

Handset server

The Handset server is required for functionality related to Avaya one-X® Mobile. It enables the Client Enablement Services server to push data to mobile clients, when the data is available and the client is also connected to the system.

Handset server manages persisted socket client connections from mobile devices and routes requests to Handset Services over a multiplexed socket. The Handset service is a part of the Client Enablement Services server. The Handset server acts as a request-response router between the mobile client and the handset services.

Handset server is installed either as a standalone installation or as a co-resident installation.

For details on Handset server installation, see *Implementing Avaya one-X® Client Enablement Services* guide.

Related topics:

[Configuring the handset server and handset service](#) on page 67

Configuring the handset server and handset service

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Handset**.
3. On the **Handset Configuration** page, enter the appropriate information and click **Update** to update the Handset service and Handset server information.

   For a coresident handset server installation, the field values in the **Handset service** and **Handset server** fields are auto populated. For a standalone handset server installation, you have to enter values in the **Handset service** fields, but do not enter any value in the **Handset server** fields. The system displays an error message if you enter values in the **Handset server** fields for a standalone handset server installation:

   ```
   The Handset Server is resident on a different location, could
   not update server configuration.
   ```

   Note:

   Do not use non SSL values for the Handset server and Handset service. You must select the **Secure Port** check box for both the Handset server and the

Handset service. Users must also select the **Secure SSL Connection** check box on the client application.

For more information on fields, see Handset Server field descriptions on page 83.

4. Click **Update** to save the field values with the changes you made.

   The handset server configuration is stored in a properties file in the following location: `/opt/avaya/HandsetServer/handset_server.properties`

   The handset service configuration is stored in a properties file in the following location: `/opt/IBM/WebSphere/AppServer70/lib/ext/HandsetServices.properties`

5. Click **Reset** to display the settings from the start of this session.

Next steps

You must restart the Handset service to save your changes. See Monitoring Handset services on page 189.

Audio Transcoding

Voice mails are generally stored in WAV (Waveform Audio File) format. Many mobile device do not support WAV format and prefer to play it in other formats such as AMR, MP3, and so on. These formats are audio compressed formats and consume less memory as compared to the WAV format. Audio transcoding server facilitates the conversion of stored voice messages to a format supported by the mobile device.

In Avaya one-X® Client Enablement Services Release 6.1, by default the Audio Transcoding server is co-resident with the Client Enablement Services server.

Audio Transcoding service accesses the Audio transcoding server for voice messages. Handset services use the Audio Transcoding service whenever a mobile client application accesses voice messages.

Related topics:

Modifying the audio transcoding server on page 69

Modifying the audio transcoding server

Procedure

1. Select the **Servers** tab.
2. From the left pane, select **Audio Transcoding**.
3. Click the name of the Audio Transcoding server in the **Handle** column to display the Modify Audio Transcoding page.
4. Enter the appropriate information and click **Save** to update the server.

   For more information on the fields, see Audio Transcoding field descriptions on page 83.
5. Click **Reset** to restore the settings to the last saved page or the default values if this is a new object.
6. Click **Cancel** to exit the page without making any changes.

Servers field descriptions

- Telephony server field descriptions on page 69
- Auxiliary server (Session Manager) field descriptions on page 73
- Voice Messaging server field descriptions on page 74
- Conferencing server field descriptions on page 78
- Presence server field descriptions on page 79
- Dial Plan field descriptions on page 81
- Handset Server field descriptions on page 83
- Audio Transcoding field descriptions on page 83
- Routing Configuration field descriptions on page 85

Telephony server field descriptions

Name	Description
Type	The type of switch configured on the system. For Communication Manager, the system displays *cm*.

Name	Description
Version	The version of the switch configured on the system.
Handle	The unique name assigned to the server by the administrator.
Description	A short description of the server that uniquely identifies the Telephony server.
Enabled	When selected, enables the telephony server for the Client Enablement Services server.
Remove ARS from dialed number before converting to display string	When Client Enablement Services makes an outgoing call, which happens in case of a call back, Communication Manager sends the called number back to Client Enablement Services for a record in the call history. If Communication Manager includes the ARS digits in the number sent to Client Enablement Services, the Client Enablement Services server uses this number to transform and display on the client application. The number displayed on the client application includes the ARS digits prefixed to the original number called from the Client Enablement Services server or is not as per the dial plan transformation rules set for the **Conversion from ANI to displayed string in client** rule. However, if the **Remove ARS from dialed number before converting to display string** check box is selected, Client Enablement Services removes the ARS digits prefix before transforming the number and displaying the number on the client application. By default, this check box is selected.
ARS prefix overlaps with extension	When internal numbers start with the same numbers used as ARS, and the **ARS prefix overlaps with extension** check box is selected, Client Enablement Services matches the dialed number with the number of digits configured for a local call. If the number length of the dialed number is smaller than the local call length, Client Enablement Services does not remove the ARS digits from outgoing calls. For example, if an internal call is starting with the ARS prefix, calls to 98710 can be

Name	Description
	interpreted as ARS + 8710 or as extension 98710. If you select this check box, the call is treated as the call made to extension 98710. **Note:** To select the **ARS prefix overlaps with extension** check box, you must select the **Remove ARS from dialed number before converting to display string** check box.
Allow Direct Connection to CM	When selected, enables the server to establish a direct connection with Communication Manager. If this field is selected and all Session Managers configured in Client Enablement Services are not available, Client Enablement Services connects directly to Communication Manager through a direct SIP trunk and Communication Manager handles all calls.
Domain	Domain of the network region. You can get the domain from the **IP Network region** table of Communication Manager, where the value is displayed as **Authoritative Domain: *sysucd.avaya.com***. You can obtain this value from the SIP Signaling Group (Far-end Domain Value) administered on Communication Manager that connects to the Client Enablement Services server or Session Manager.
SIP Remote Host	SIP remote host is a Communication Manager Ethernet interface that is configured as the Near-end node in the Communication Manager signaling group configuration to communicate with Client Enablement Services server. **Note:** If you configure Communication Manager as Processor Ethernet (PE), enter the IP address of the PROCR interface of Communication Manager.
SIP Remote Port	The port used by Communication Manager to talk to the Client Enablement Services server.

Name	Description
	For a secure connection using TLS, this port should be set to 5061.
SIP Remote Secure	When selected, uses a secure port for SIP services on the Client Enablement Services server.
Session Manager - Available	The handle of the Session Manager servers configured on Client Enablement Services. Select a server and click **Add** to move it to the **Selected** field.
Session Manager - Selected	The handle of the Session Manager servers selected for this Telephony server. Select a server and click **Remove** to move it to the **Available** field.
Dial Plan	The handle of the Dial Plan used by this server. If you do not select a Dial Plan, the outgoing numbers do not get transformed into the dialable format of Communication Manager. Users cannot dial numbers from Call Logs or Contacts.
OK or **Save**	**OK** used on Add/Create pages saves the new resource. **Save** on Modify pages saves updates to the resource.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Removes the server from Client Enablement Services.
Test	Tests the new or updated server settings and gives the results immediately. In case of an error, you can make the necessary corrections at once.
Synchronize	Synchronizes the dial plan and routing configuration changes with the mobile number information stored on Communication Manager.

Auxiliary server (Session Manager) field descriptions

Name	Description
Type	The type of server configured on the system. For Session Manager, the system displays *sm*.
Version	The version of the server configured on the system.
Handle	The unique name assigned to the server by the administrator.
Description	A short description of the server that uniquely identifies the Session Manager configured in the Client Enablement Services server.
Enabled	When selected, enables the telephony server for the Client Enablement Services server.
Domain	SIP routing domain as configured in Session Manager.
SIP Address Host	IP address of the asset card of Session Manager.
SIP Address Port	The port used by Session Manager to talk to the Client Enablement Services server.
OK or **Save**	**OK** used on Add/Create pages saves the new resource. **Save** used on Modify pages saves updates to the resource.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Removes the server from Client Enablement Services.
Test	Tests the new or updated server settings and gives the results immediately. In case of an error, you can make the necessary corrections at once.

Voice Messaging server field descriptions

Name	Description
Type	The type of server configured on the system. For the Modular Messaging server, displays MM.
Version	The version of the server configured on the system.
Handle	The unique name assigned to the server by the administrator.
Description	A short description of the server that uniquely identifies the Voice Messaging server.
Enabled	When selected, enables the telephony server for the Client Enablement Services server.
Encoding Type	Encoding type for the voice messaging files. The supported encoding types are **GSM** and **G.711**. For more information about GSM and G.711, see the *Administering Avaya Aura® Messaging* guide.
Initial Number of Server Connections	The minimum number of Client Enablement Services user connections needed to communicate with the storage server of the messaging server. The default of this field is 50. If you are configuring Communication Manager Messaging as the voice messaging server, set the value of this field to 10. Setting this field to a lower value makes the voice messaging adaptor respond quickly.
Max Number of Server Connections	The maximum number of Client Enablement Services server connections that can be assigned to the Voice Messaging server. The default value is 200, the maximum number of connections allowed is 2200.
Client Connections Increment	The number of times to increment the connections based on the number of users in the connections. For example, if this value is 2 and there are 100 users per connection, the connections increments for every 200 users.
Users Per Client Connection	The number of users assigned per connection to the Voice Messaging server.

Name	Description
Messages Temp Directory	The location of the temporary directory where sections of voice mail message are stored. When creating a new Voice Messaging server, enter either the name of the default directory `/msgWorkDir` or the name of the directory you created for the Voice Messaging server. See Creating a directory for the Voice Messaging server on page 55.
Temp Purge Interval	The number of minutes that the sections of voice mail messages can remain in storage before the temporary directory is purged and the sections are deleted.
Mail Domain	The fully qualified domain name of the storage server of the messaging server.
SSL Certificate	Indicator for an SSL Certificate for this server. • Displays **Remove SSL Certificate** if the security certificate exists for this server. • Click **Retrieve SSL Certificate** if the security certificate for this server is not found. The security certificate is retrieved for the server.
Dial Plan	The handle of the Dial Plan used by this server. The dial plan you select on the Voice Messaging Server page is used for conversion of the number from the messaging server to be displayed for the visual voice mail number on the Avaya one-X® Mobile client application.
IMAP Host	The network address of the storage server of the messaging server. This field must include an IP address, not a fully qualified domain name.
IMAP Port	The secure port number used by the **IMAP** configuration for the Voice Messaging server. 993 is the default port for SSL.
IMAP Login ID	The secure log-in ID used by the **IMAP** configuration for the Voice Messaging server.

Name	Description
	This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
IMAP Password	The secure password associated with the log-in ID used by the **IMAP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in your Voice Messaging server.
IMAP Confirm	Verification of the password associated with the log-in ID used by the **IMAP** configuration for the messaging server.
IMAP Secure Port	If you select this option, Client Enablement Services requires a secure **IMAP** connection for the Voice Messaging server. Verify that this port is the correct port for a secure connection.
SMTP Host	The network address of the storage server of the messaging server. This field must include an IP address, not a fully qualified domain name.
SMTP Port	The port number used by the **SMTP** configuration for the Voice Messaging server. 25 is the default port.
SMTP Login ID	The secure log-in ID used by the **SMTP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
SMTP Password	The secure password associated with the log-in ID used by the **SMTP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in the Voice Messaging server.
SMTP Confirm	Verification of the password associated with the log-in ID used by the **SMTP** configuration for the messaging server.
SMTP Secure Port	If selected, indicates **SMTP** is configured to use a secure connection for the Voice Messaging server.

Name	Description
	A secure **SMTP** connection to the Voice Messaging server is optional.
LDAP **Host**	The network address of the storage server of the messaging server. This field must include an IP address, not a fully qualified domain name.
LDAP **Port**	The port number used by the **LDAP** configuration for the Voice Messaging server. 636 is the default port.
LDAP **Login ID**	The log-in ID used by the **LDAP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
LDAP **Password**	The password associated with the log-in ID used by the **LDAP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in the Voice Messaging server.
LDAP **Confirm**	Verification of the password associated with the log-in ID used by the **LDAP** configuration for the messaging server.
LDAP **Secure Port**	Do not select this field. Client Enablement Services does not support a secure **LDAP** connection for the Voice Messaging server.
OK or **Save**	**OK** used on Add/Create pages saves the new resource. **Save** used on Modify pages saves updates to the resource.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Removes the server from Client Enablement Services.

Name	Description
Test	Tests the new or updated server settings and gives the results immediately. In case of an error, you can make the necessary corrections at once.

Conferencing server field descriptions

Name	Description
Type	The type of server configured on the system. For Conferencing, the system displays MX.
Version	The version of the server configured on the system.
Handle	The unique name assigned to the server by the administrator.
Description	A short description of the server that uniquely identifies the Conferencing server.
Enabled	When selected, enables the telephony server for the Client Enablement Services server.
BCAPI Logger Directory	The path name of the directory where information about **BCAPI** issues is stored. See Creating a directory for the Conferencing server on page 59.
Dial Plan	The handle of the Dial Plan used by this server. This feature is not supported in this release. Do not configure a dial plan for the Conferencing server.
BCAPI Host	The network address that the **BCAPI** configuration uses for the Conferencing server as an IP address or a DNS address.
BCAPI Login ID	The log-in ID that the **BCAPI** configuration uses for the Conferencing server. The number of characters in this entry must not exceed the character length limitation in **BCAPI**.
BCAPI Password	The password associated with the log-in ID that the **BCAPI** configuration uses for the Conferencing server. The number of characters in this entry must not exceed the character length limitation in **BCAPI**.

Name	Description
BCAPI **Confirm**	Verification of the password associated with the log-in ID used by the **BCAPI** configuration for the Conferencing server.
BCAPI **Secondary Login ID**	The **Secondary Login ID** used by the **BCAPI** configuration for the Conferencing server.
BCAPI **Password**	The password associated with the **Secondary Login ID** used by the **BCAPI** configuration for the Conferencing server.
BCAPI **Confirm**	Verification of the password associated with the secondary log-in ID used by the **BCAPI** configuration for the Conferencing server.
OK or **Save**	**OK** used on Add/Create pages saves the new resource. **Save** used on Modify pages saves updates to the resource.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Removes the server from Client Enablement Services.
Test	Tests the new or updated server settings and gives the results immediately. In case of an error, you can make the necessary corrections at once.

Presence server field descriptions

Name	Description
Type	The type of server configured on the system. For the Presence Services, the system displays *ps*.
Version	The version of the server configured on the system.
Handle	The unique name assigned to the server by the administrator.
Description	A short description of the server that uniquely identifies the Presence Services.

Name	Description
Enabled	When selected, enables the telephony server for the Client Enablement Services server.
PS Publish To Port	The port number on the Presence Services server where the presence information of the user is published.
PS Consumer Port	The port number on the Presence Services server that receives the consumer information.
PS Supplier Port	The port number on the Presence Services server that furnishes the published the information.
Web service Port	Web Service port is the port Client Enablement Services uses for presence related communication with System Manager.
RMI Export Port	Replication listener is exported on the RMI export port. The exported objects are authorization request call-backs. The default value of the port is 2009. You can also set this port to 0, if you want the system to select the available port.
RMI Registry Port	RMI register listens on the RMI registry port. The default value of the port is 2009.
RMI Secure Port	When selected, makes the replication related RMI communication secure. Clear this check box only if you want the communication to be insecure. This requires Presence Services adjustments.
Presence Services (PS) Host	The network host address of Presence Services. It can be defined either as FQDN (fully qualified domain name), or as an IP address.
Presence Services (PS) Port	The SIP service communication port between Client Enablement Services and Presence Services.
Management Service (SMGR) Host	The network host address of System Manager. It can be defined either as FQDN or as an IP address.

Name	Description
	Note: The System Manager IP should be the same as the System Manager IP mentioned in the pre-install plug in during the installation of the Client Enablement Services server.
Management Service (SMGR) Port	TCP/IP port used for LPS to communicate with System Manager. This is set by default unless this is changed inSystem Manager.
Management Service (SMGR) Login ID	The log-in ID used by System Manager for the presence server.
Management Service (SMGR) Password	The password associated with the log-in ID used by System Manager for the presence server.
Confirm	Verification of the password associated with the log-in ID used by System Manager for the presence server.
OK or **Save**	**OK** used on Add/Create pages saves the new resource. **Save** used on Modify pages saves updates to the resource.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Removes the server from Client Enablement Services.

Dial Plan field descriptions

Name	Description
Handle	The unique name assigned to the server by the administrator.
Phone Numbers **PBX Main**	A sample of a valid telephone number on the switch. The Dial Plan compares this number with other telephone numbers to determine whether a telephone number is internal or external.

Name	Description
Phone Numbers **Automatic Routing Service**	The digit to prefix before an outbound phone number is dialed on the PBX. For example, in the phone number 9-1-800-8888, 9 is the **Automatic Routing Service** number.
Prefixes **Regional**	The area code of the region.
Prefixes **Inter-Regional**	The digit to dial between area codes in an **Inter-Regional** phone call.
Prefixes **International**	The digits to prefix to place an **International** phone call. For example, in the phone number 011-1-800-8888, 011 is the **International** prefix code.
Number of Digits **National Call Maximum**	The maximum number of digits allowed in a domestic telephone call. For example, if the phone number is 508-852-0010, the value is 10.
Number of Digits **Local Call**	The maximum number of digits in a telephone call within an area code. For example, if the phone number is 508-852-0010, the value is 10.
Number of Digits **Extension to Extension Call**	The maximum number of digits allowed in a phone extension at the enterprise. Typically, this value is 7 or less.
OK or **Save**	**OK** used on Add/Create pages saves the new resource. **Save** used on Modify pages saves updates to the resource. See Dial Plan services on page 22 for more details.
Reset	On Modify/Update pages, restores the form values back to the last successfully saved page. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Removes the server from Client Enablement Services.
Test	Tests the new or updated server settings and gives the results immediately. In case of an

Name	Description
	error, you can make the necessary corrections at once.

Handset Server field descriptions

Name	Description
Handset service Listening port	Port on which the Handset service listens for connections from the Handset server. The default value of this field is 8888.
Handset service Secure Port	When selected makes the port number used by the Handset service secure. Do not use non SSL value for the Handset service. You must select the **Secure Port** check box for the Handset service.
Handset server Host	IP address of the Handset server.
Handset server Secure Port	When selected makes the port number used by the Handset server secure. Do not use non SSL value for the Handset server. You must select the **Secure Port** check box for the Handset server.
Handset server Listening port	Port on which the Handset server listens for connections from the mobile clients. The default value of this field is 7777.
Handset server Handset service host	IP address of the Handset service on Client Enablement Services to which the Handset server connects.
Handset server Handset service port	Ports on which the Handset services listen for connections from the Handset server.
Update	Updates the page with the modified information.
Reset	Restores the form values back to the last successful save.

Audio Transcoding field descriptions

Name	Description
Type	Type of the Audio Transcoding service.
Version	Version of the Audio Transcoding service.
Handle	The unique name assigned to the Audio Transcoding service by the administrator.

Name	Description
Description	A short description of the Audio Transcoding service.
Enabled	When selected, enables the Audio Transcoding service for the system.
Request time-to-live (seconds)	The maximum time a client request for transcoding a file is kept on hold, after which the client request is marked as failed. The default value of this field is 20.
Max number of pending requests	Maximum number of requests that can be pending to the transcoding server. The default value of this field is 1000.
Max server cache size	The maximum cache size allowed on the shared storage location. The unit of this field is in Megabyte (MB). The default value of this field is 1000.
Cache cleanup frequency (seconds)	The frequency of cache cleanup from the shared storage location. The default value of this field is 300.
Cache cleanup percentage	The percentage of audio cache files which are cleaned up from the shared storage location. The default value of this field is 75.
Max cache age (seconds)	The maximum duration for which a cache file can remain unclean from the shared storage location. The default value of this field is 86400.
Destination of converted audio messages	The shared storage location where the transcoding server caches the converted audio files. The default value of this field is `/tmp/transcoding`.
Pending transactions limit	The maximum limit of transactions pending with the transcoding server. The default value of this field is 500.
Alert threshold for pending transactions	The number of pending transaction after which the transcoding server gives an alert. The default value of this field is 400.
Server threads pool size	Number of threads in a pool for conversion by the server. The default value of this field is 10.
Transcoding Server Address: Host	IP address of the transcoding server.

Name	Description
Transcoding Server Address: Port	Port number which the transcoding server uses. The default value of this field is 8090.
Save	Saves the changes made to the audio transcoding server.
Reset	Restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.

Routing Configuration field descriptions

Name	Description
Type	Type of the routing configuration. • For location routing, **Type** is **Location**. • For mobile routing, **Type** is **GSM Gateway**. • For additional destination routing, **Type** is **Mobile/Ring also Location**.
Name	Name of the routing configuration.
CM Location ID	A unique location ID of Communication Manager. Communication Manager supports multiple locations and it identifies a network region by its Location ID. Based on the location ID, the Dial Plan formats the telephone number of a user.
Dial Plan	The handle of the Dial Plan used by this server.
Prefix	The number prefixed to the dialable number. **Note:** This field is available only for the **GSM gateway**.
Description	A short description of the routing configuration.

Chapter 4: User administration

System Profile

The System Profile is a collection of the following properties applicable to groups that are members of the system.

- **Send DTMF for calls**
- **Enforce Call Handling on BlackBerry Clients**
- **DTMF detection for callback**
- **DTMF detection for inbound calls**
- **Extension Contact Logging (SipService)**
- **Forward voice messages to inbox**
- **Save to voice messages file**
- **Maximum voice messages**
- **Conference Contact Logging**
- **Maximum number of history records**
- **Maximum days to keep history**
- **Maximum number of favorites**
- **Contact Logging (Exchange Contact Service)**
- **Usage Disclaimer**
- **Usage Disclaimer URL**
- **Feedback Email Address**
- **Maximum number of entries per portal view**
- **Allow voice messages on mobile**
- **Require login each time one-X Mobile is launched on mobile device**
- **Require client software upgrades**
- **Number of days to warn users before making updates mandatory**
- **Speech Access Number**

Note:

Forward voice messages to inbox, **Save to voice messages file**, **Contact Logging (Exchange Contact Service)**, **Usage Disclaimer**, **Usage Disclaimer URL**, **Feedback Email Address**, and **Maximum number of entries per portal view** properties are not supported in Avaya one-X® Client Enablement Services release 6.1.2

Avaya one-X® Client Enablement Services provides one System Profile which you can modify to apply its property values to all users and groups on the system. For System Profile properties, you can accept the default value, set a new system value, or force the value at the Group Profiles level. By default all provisioned users are assigned the System Profile properties, unless you assign a Group Profile to them.

Important:

At the system and group levels, **Force Value In Groups** does not affect the Presence settings. User settings override the forced system level settings.

Related topics:

Displaying the System Profile on page 88
Modifying the System profile on page 88
Users field descriptions on page 120

Displaying the System Profile

Procedure

1. Select the **Users** tab.
2. From the left pane, select **System Profile**.
   The System Profile page displays the System Profile properties.

Related topics:

System Profile on page 87
Users field descriptions on page 120

Modifying the System profile

Procedure

1. Click the **Users** tab.
2. In the left pane, click **System Profile**.

3. On the System Profile page, modify the values of the system profile properties as needed.

   You can accept the default values for these properties or set new values. You can also force the value of the property to any Group profile that uses this property.

   - If you set the **System Value** as **Accept default** and if you do not specify a **Group Value**, it is set as the **Default** value of the **System Profile**.
   - If you set the **System Value** as **Set System Value**, and if you do not specify a **Group Value**, it is set as the value as specified in the **System Profile**.
   - If you set the **System Value** as **Force Value in Groups**, the **Group Value** is set as the **System Value** as specified in the **System Profile** even if you specify a different value in the **Group Profile**.
4. Click **Save** to save these settings to the profile.
5. Click **Reset** to display the settings from the start of this session.

Related topics:
System Profile on page 87
System profile and Group profile field descriptions on page 92
Users field descriptions on page 120

Group Profiles page

A Group profile is a collection of the following properties applicable to users who are members of the group.

- **Send DTMF for calls**
- **Enforce Call Handling on BlackBerry Clients**
- **DTMF detection for callback**
- **DTMF detection for inbound calls**
- **Extension Contact Logging (SipService)**
- **Forward voice messages to inbox**
- **Save to voice messages file**
- **Maximum voice messages**
- **Conference Contact Logging**
- **Maximum number of favorites**
- **Contact Logging (Exchange Contact Service)**

- **Usage Disclaimer**
- **Usage Disclaimer URL**
- **Allow voice messages on mobile**
- **Require login each time one-X Mobile is launched on mobile device**
- **Require client software upgrades**
- **Number of days to warn users before making updates mandatory**
- **Speech Access Number**

Note:

Forward voice messages to inbox, **Save to voice messages file**, **Contact Logging (Exchange Contact Service)**, **Usage Disclaimer**, and **Usage Disclaimer URL** properties are not supported in Avaya one-X® Client Enablement Services release 6.1.2

Use a Group profile to apply values to the users in the group who use the same properties. When you set values that are forced from the system level, Group profiles inherit values from System profiles. Forced values are system-level values that cannot be changed at the lower Group profile or user profile levels. If the values are not forced from the system level, you can either accept the system level value for a Group profile or override it with a group value.

Related topics:

Adding group profiles on page 90
Listing group profiles on page 91
Modifying group profiles on page 91
Deleting group profiles on page 92
System profile and Group profile field descriptions on page 92
Users field descriptions on page 120

Adding group profiles

Procedure

1. Select the **Users** tab.
2. From the left pane, select **Group Profiles**.
3. On the Group Profiles page, click **Add New Group Profile** to display the Create a New Group Profile page.

   Note:

   You can add maximum 500 Group profiles.
4. Enter the name of the profile in the **Handle** field.
5. Enter a brief description of the profile in the **Description** field.

6. Set the properties in the Group profile as needed.

   You can accept the system default value or set a new Group profile value. If the value of the property is forced from the System profile, you cannot change that value.
7. Click **OK** to create the profile.
8. Click **Reset** to display the settings from the start of this session.
9. Click **Cancel** to exit the page without making any changes.

Related topics:

Group Profiles page on page 89

Users field descriptions on page 120

Listing group profiles

Procedure

1. Click the **Users** tab.
2. From the left pane, select **Group Profiles**.
   The Group Profiles page displays a list of the Group profiles on the system.

Related topics:

Group Profiles page on page 89

Users field descriptions on page 120

Modifying group profiles

Procedure

1. Select the **Users** tab.
2. From the left pane, select **Group Profiles**.
3. On the Group Profiles page, click the **Handle** field for a profile to display the Modify Group Profile page for the profile.
4. Modify the Group profile properties as required.

   You can accept the system default value or set a new Group Profile value. If the value of the property is forced from the System Profile, you cannot change that value.

5. Click **Save** to save the settings to the profile.
6. Click **Reset** to display the settings from the start of this session.
7. Click **Cancel** to exit the page without making any changes.

Related topics:

Group Profiles page on page 89
System profile and Group profile field descriptions on page 92
Users field descriptions on page 120

Deleting group profiles

Procedure

1. Click the **Users** tab.
2. From the left pane, select **Group Profiles**.
3. Click the name of a Group profile in the **Handle** field to display the Modify Group Profile page for the profile.
4. Click **Delete** to delete the Group profile.

System profile and Group profile field descriptions

Property	Description
Send DTMF for calls	If **Disabled**, turns off the **Send DTMF for calls** option when in a call.
Enforce Call Handling on BlackBerry Clients	If **Enabled**, users with the Avaya one-X® Mobile client application installed on a BlackBerry mobile device always stay connected with the Client Enablement Services server. This feature forces all calls made from this BlackBerry mobile device to go through the Client Enablement Services server and prohibits the user from making calls using the service provider’s network except emergency calls. When this feature is enabled, following features get enabled on the Avaya one-X®

Property	Description
	Mobile client application installed on a BlackBerry mobile device: • A user is automatically logged in the Avaya one-X® Mobile client application as soon as the user switches on the BlackBerry mobile device. • The **Exit Application** option is unavailable. • The **Use one-X Mobile for All calls** option is always selected, and user cannot change this configuration. ✱ **Note:** If this feature is required for BlackBerry users, such users must install the Avaya one-X® Mobile client application available with Client Enablement Services Release 6.1SP1.Avaya one-X® Mobile Release 6.1.2 does not support the Enforce call handling feature.
DTMF detection for callback	Select **Enabled** if Communication Manager should wait for a DTMF tone before considering that the user answered the phone in a callback. The callback initiated by Communication Manager is complete when the mobile handset transmits the confirmation DTMF tone.
DTMF detection for inbound calls	Select **Enabled** if Communication Manager should wait for a DTMF tone before considering that the user answered the phone in a callback. The incoming calls to Communication Manager are complete when the mobile handset transmits the confirmation DTMF tone.
Extension Contact Logging (SipService)	**off**. Never records the call log. **24*7**. Records the contact log always even when the user is not logged in.
Forward voice messages to inbox	If **Enabled**, forwards the voice messages received by a user on Client Enablement Services to the e-mail inbox of the user. This field is not supported in Client Enablement Services Release 6.1 SP3.

Property	Description
Save to voice messages file	If **Enabled**, saves the voice messages received by a user on Client Enablement Services to the voice messages file. This field is not supported in Client Enablement Services Release 6.1SP3.
Maximum voice messages	Maximum number of voice messages that a user can save. When the number of voice message starts reaching the maximum number defined for a user, the user gets a warning. The default value is 50. Enter a value between **1** and **400**. In the Avaya one-X® Mobile client application, users can view only 15 voice messages at a time on their mobile device. If there are more than 15 voice messages on the server, they have to delete one message to receive the next one. Messages are listed on a first in first out basis. If a new voice message arrives, the client application removes the oldest message from the list to display the new one.
Conference Contact Logging	**on**. Records the conference log only when the user is logged in. **off**. Never records the conference log. **24*7**. Records the conference log always even when the user is not logged in.
Maximum number of entries per portal view	This is only a System profile field. Maximum number of entries allowed per portal view on Client Enablement Services. Enter a value between **1** and **200**. This field is not supported in Client Enablement Services Release 6.1SP3.
Maximum number of history records	This is only a System profile field. Maximum number of records to archive on Client Enablement Services. Enter a value between **1** and **400**.
Maximum days to keep history	This is only a System profile field. Maximum number of days to keep these records in archive on Client Enablement Services. Enter a value between **1** and **14** days.
Maximum number of favorites	Maximum number of favorites a Client Enablement Services user can save on their client application. Enter a value between **1** and **5000**.

Property	Description
Contact Logging (Exchange Contact Service)	**off**. Never records the contact log. **24*7**. Always records the contact log. This field is not supported in Client Enablement Services Release 6.1SP3.
Usage Disclaimer	**Enabled**. Turns on the **Usage Disclaimer** on Client Enablement Services. This field is not supported in Client Enablement Services Release 6.1SP3.
Usage Disclaimer URL	URL for the **Usage Disclaimer** on Client Enablement Services. The default value is **usage.jsp**. This field is not supported in Client Enablement Services Release 6.1SP3.
Feedback e-mail address	This is only a System profile field. E-mail address for the user to provide feedback to the Client Enablement Services administrator. This field is not supported in Client Enablement Services Release 6.1SP3.
Allow voice messages on mobile	**Enabled**. Allows sending voice messages to the mobile of the user.
Require login each time one-X Mobile is launched on mobile device	If **Enabled**, the Avaya one-X® Mobile client application does not store the login credentials of the user on the mobile device for added security. The user needs to manually log in each time the client application is launched or when the client application has to reconnect during a normal operation.
Require client software upgrades	If **Enabled**, allows the user to receive Client Enablement Services software upgrades notifications.
Number of days to warn users before making updates mandatory	Number of days before which the end user gets a system generated warning to make the update. The system performs the update after the specified the number of days have passed. The default value is 15. Enter a value between **1** and **100**.
Speech Access Number	There is no default value for this field. You have to enter the default value. Enter a value in this field only if the customer has the Speech Access application set up. In this field, enter the DID that the Avaya one-X®

Property	Description
	Mobile client application can use to access the Speech Access application.

Related topics:

Modifying the System profile on page 88
Modifying group profiles on page 91

Prototype Users

A Prototype user is a collection of configuration settings and service provisioning values that you can apply to other users while provisioning a user. You can use Prototype users as templates to speed up the configuring and provisioning of users, who have similar settings.

Note:

Use Prototype users for provisioning users only. The resources you have assigned to a prototype user are copied to the users you are provisioning. Once you provision a user using a prototype user, any change made to the Prototype user does not impact the users that are provisioned using this Prototype user.

Related topics:

Adding Prototype users on page 96
Listing Prototype users on page 97
Assigning a Telephony resource to a Prototype User on page 98
Assigning a Mobile Telephony resource to a Prototype User on page 98
Assigning a Voice Messaging resource to a Prototype User on page 99
Assigning a Conferencing resource to a Prototype User on page 100
Assigning a Presence resource to a Prototype User on page 101
Modifying Prototype Users on page 101
Users field descriptions on page 120

Adding Prototype users

Procedure

1. Select the **Users** tab.
2. From the left pane, select **Prototype Users**.
3. On the Prototype Users page, click **Create Prototype User** to display the Create Prototype User page.

4. In the **Handle** field, enter the name of the Prototype user.
5. In the **Description** field, enter a short description of the name of the Prototype user.
6. Click **Continue** to save these fields.
7. Add the following resources to the Prototype user:
    - Telephony resource. Perform the steps in Assigning a Telephony resource to a Prototype User on page 98.
    - Mobile telephony resource. Perform the steps in Assigning a Mobile Telephony resource to a Prototype User on page 98.
    - Messaging resource. Perform the steps in Assigning a Voice Messaging resource to a Prototype User on page 99.
    - Conferencing resource. Perform the steps in Assigning a Conferencing resource to a Prototype User on page 100.
    - Presence resource. Perform the steps in Assigning a Presence resource to a Prototype User on page 101.

    Note:

    When you provision a user using this Prototype user, you must add a Personal Contact resource to the user if the user is using the Avaya one-X® Communicator client application. However, for users using Avaya one-X® Communicator Release 6.1 SP3, do not add a personal contact resource.
8. Click **Finished** to save the Prototype User.
9. Click **Delete** to remove the Prototype User.

Related topics:

Prototype Users on page 96

Assigning a Personal contact resource to a user on page 119

Users field descriptions on page 120

Listing Prototype users

Procedure

1. Select the **Users** tab.
2. From the left pane, select **Prototype Users**.
   The system displays the Prototype users on the system.

Related topics:

Prototype Users on page 96

Users field descriptions on page 120

Assigning a Telephony resource to a Prototype User

About this task

If you are creating a new Prototype User and have already assigned a **Handle** and **Description** to the user, and now you want to add a telephony resource to a user, go to step 4.

Procedure

1. Select the **Users** tab.
2. From the left pane, select **Prototype User**.
3. Click the link in the **Handle** column for the Prototype User you want to assign the telephony resource.
4. In the **Telephony** group box, click **Add**.
5. Complete the following fields:
    a. From the **Server** drop-down list, select the handle of the Communication Manager server.
    b. In the **Display Name** field, type a descriptive name for this resource which users see in the Avaya one-X® Client Enablement Services.
    c. From the **Destination Routing** drop-down list, select a destination routing you want to configure for this telephony resource.
6. Click **Save**.
   The browser returns to the Prototype User page.

Assigning a Mobile Telephony resource to a Prototype User

Before you begin

Before you add a Mobile telephony resource to a user, you must add a Telephony resource for the user.

About this task

If you are creating a new Prototype user and have already assigned a **Handle** and **Description** to the user, and now you want to add a mobile telephony resource to a user, go to step 4.

Procedure

1. Select the **Users** tab.
2. From the left pane, select **Prototype User**.
3. Click the link in the **Handle** column for the Prototype User you want to assign the telephony resource.
4. In the **Mobile Telephony** group box, click **Add**.
5. Complete the following fields:
    a. In the **Display Name** field, type a descriptive name for the mobile telephony resource which users see in the Avaya one-X® Client Enablement Services.
    b. From the **Mobile Routing** drop-down list, select a routing configuration for this telephony resource. The incoming calls are routed to a mobile number based on the Mobile routing configured for the user.
    c. From the **Ring-also Routing** drop-down list, select a routing configuration for this telephony resource. The system routes the incoming calls to a number other than the mobile number based on the Ring-also routing configured for the user.
    d. From the **Callback Routing** drop-down list, select a routing configuration for this telephony resource. The system routes the calls to a number specified by the user for callback based on the routing configuration selected for callback.
6. Click **Save**.
   The browser returns to the Prototype User page.

Assigning a Voice Messaging resource to a Prototype User

About this task

If you are creating a new Prototype user and have already assigned a **Handle** and **Description** to the user, and now you want to add a voice messaging resource to a user, go to step 4.

Procedure

1. Select the **Users** tab.
2. In the left navigation pane, select **Prototype Users**.
3. Click the link in the **Handle** column for the Prototype User you want to assign the voice messaging resource.
4. In the **Voice Messaging** group box, click **Add**.
5. Complete the following fields:
    a. From the **Server** drop-down list, select the handle of the messaging server.

   b. In the **Display Name** field, type a descriptive name for this messaging resource which users see in the Avaya one-X® Client Enablement Services.
   c. In the **Web Subscriber Options URL** field, enter the URL of Web Subscriber Options service of the Modular Messaging server from where users can make changes to their voice mailbox settings such as when the message waiting indicator comes on.

      Enter the URL in the **Web Subscriber Options URL** field, only if you are using a Modular Messaging server as the messaging server. The **Web Subscriber Options URL** field is not available if the voice messaging server is either Avaya Aura® Messaging or Communication Manager Messaging.
   d. From the **SMS notification** drop-down list, select **All**, **None**, or **Priority**. If SMS Notification is set to **None**, user does not receive any notification of a new voice mail. If SMS Notification is set to **All**, user receives notifications for all new voice mails. If SMS Notification is set to **Priority**, user receives notifications of voice mails from contacts marked as priority.

6. Click **Save**.
   The browser displays the Prototype User page.

Assigning a Conferencing resource to a Prototype User

About this task

If you are creating a new Prototype user and have already assigned a **Handle** and **Description** to the user, and now you want to add a conferencing resource to a user, go to step 4.

Procedure

1. Select the **Users** tab.
2. In the left navigation pane, select **Prototype Users**.
3. Click the link in the **Handle** column for the Prototype User you want to assign the conferencing resource.
4. In the **Conferencing** group box, click **Add**.
5. Complete the following fields:
   a. From the **Server** drop-down list, select the handle of the Conferencing server.
   b. In the **Display Name** field, type a descriptive name for this resource that users will see in the Avaya one-X® Client Enablement Services.
   c. In the **Bridge Number** field, type the telephone number that the user dials to log in to the bridge.
   d. In the **Bridge Number Backup** field, type the secondary telephone number that the user can dial to log in to the bridge.

    e. Select the **Allow Call Me** check box.

6. Click **Save**.
   The browser returns to the Prototype User page.

Assigning a Presence resource to a Prototype User

About this task

If you are creating a new Prototype user and have already assigned a **Handle** and **Description** to the user, and now you want to add a presence resource to a user, go to step 4.

Procedure

1. Select the **Users** tab.
2. In the left navigation pane, select **Prototype Users**.
3. Click the link in the **Handle** column for the Prototype User you want to assign the presence resource.
4. In the **Presence Information** group box, click **Add**.
5. Complete the following fields:
    a. From the **Server** drop-down list, select the handle of the Presence server.
    b. In the **Display Name** field, type a descriptive name for this resource which users see in the Avaya one-X® Client Enablement Services.
6. Click **Save**.
   The browser returns to the Prototype User page.

Modifying Prototype Users

Procedure

1. Select the **Users** tab.
2. From the left pane, select **Prototype Users**.
3. On the Prototype Users page, click the name of a Prototype user in the **Handle** field to display that Prototype User page.
4. If you want to change the **Handle** or **Description** of the Prototype user, click **Update** in the Handle/Description section of the page.

   a. In the **Handle** field, enter the updated name of the Prototype user.
   b. In the **Description** field, update the description of the Prototype user.
   c. Click **Save** to save your changes.

5. Click **Update** in the resource section you want to modify:
   - Telephony resource. Perform the steps in Assigning a Telephony resource to a Prototype User on page 98.
   - Mobile telephony resource. Perform the steps in Assigning a Mobile Telephony resource to a Prototype User on page 98.
   - Messaging resource. Perform the steps in Assigning a Voice Messaging resource to a Prototype User on page 99.
   - Conferencing resource. Perform the steps in Assigning a Conferencing resource to a Prototype User on page 100.
   - Presence resource. Perform the steps in Assigning a Presence resource to a Prototype User on page 101.
6. Click **Cancel** to exit the page without making any changes.

Related topics:

Prototype Users on page 96
Users field descriptions on page 120

Avaya one-X® Client Enablement Services users configuration

Client Enablement Services users must be listed in the Enterprise Directory. The Enterprise Directory administrator should first list these users in the Client Enablement Services user group in the Enterprise Directory.

After this, you should synchronize the Enterprise Directory with the Client Enablement Services server to fetch the users listed in the Client Enablement Services user group. If the synchronization is successful, these users are listed in the unprovisioned users list in Client Enablement Services. You can now provision the unprovisioned users from the Client Enablement Services administration application.

Only after you provision the users, they can access the Client Enablement Services client applications.

Unprovisioned users

Users who are in the Client Enablement Services user group of the Enterprise Directory but have not been provisioned on Client Enablement Services.

Provisioned users

Users who are in the Client Enablement Services user group of the Enterprise Directory and are provisioned through Client Enablement Services. These users have access to client applications such as Avaya one-X® Mobile.

Related topics:

Provisioning an unprovisioned user on page 103
Listing provisioned users on page 104
Modifying provisioned users on page 106
Modifying provisioned user groups on page 106
Deleting provisioned users on page 107
Enabling or disabling a user account on page 108
Logging off and Killing user sessions on page 109
Checklist for assigning resources to a user on page 109
Assigning a Telephony resource to a user on page 111
Assigning a Mobile Telephony resource to a user on page 113
Assigning a Voice Messaging resource to a user on page 115
Assigning a Conferencing resource to a user on page 117
Assigning a Presence resource to a user on page 118
Assigning a Personal contact resource to a user on page 119
Users field descriptions on page 120

Provisioning an unprovisioned user

About this task

You can also use the Administration Command Line Interface to provision users on Avaya one-X® Client Enablement Services.

Note:

To add a user to Client Enablement Services, the user must first be a member of the users group in the enterprise directory.

To perform a bulk import of users using the CLI, see Import users on page 198.

Procedure

1. Select the **Users** tab.
2. In the left navigation pane, select **Unprovisioned Users**.

   You can search the unprovisioned users on the Client Enablement Services system on the Unprovisioned Users page.
3. You can search a user to provision the user or you can get a list of all the unprovisioned users.

- If you want to search a user and know the user ID of the unprovisioned user, go to step 4.
- If you do not know the user ID of the unprovisioned user, go to step 5.

4. Enter the user ID in the **Direct To Enterprise Directory** section and click **Provision** to provision that user.
5. Select one of the following criteria from the **Search By** drop-down list and press **Search** to display a list of users that match the criteria.
    - **Any**
    - **User ID**
    - **Display Name**
    - **First Name**
    - **Last Name**
    - In the **Pattern** field, you can enter a pattern search for the option you selected in the **Search By** drop-down list. The **Pattern** field is active after you make a selection in the **Search By** drop-down list. If you select **Last Name** in the **Search By** drop-down list and enter `sm*` in the **Pattern** field, the search result displays the name of all users whose last name starts with *sm*. One or more wildcards can be used anywhere in the search pattern.
6. Click **Provision** in the **Action** column of the user you have to provision.
7. On the Provision User page, assign a Group profile and Prototype user to the user.
8. Select **Enable**.
9. Click **Save**.
   The system displays a message: `User has been provisioned successfully.`

Related topics:

[Avaya one-X Client Enablement Services users configuration](#) on page 102
[Users field descriptions](#) on page 120

Listing provisioned users

Procedure

1. Select the **Users** tab.
2. From the left pane, select **Provisioned Users**.

The system displays the various criteria you can use to search a provisioned user.

3. Search by the following criteria and click **Search** to display a list of the desired users.
   - In the **Search By** drop-down list, the options are:
     - **Any**
     - **User ID**
     - **Last Name**
     - **First Name**
     - **Extension**
     - **Employee Number**
   - In the **Pattern** field, you can enter a pattern search for the option selected in the **Search By** drop-down list. The **Pattern** field is active only you select an option from the **Search By** drop-down list. An example of a pattern is using * to sort the list of users by last name when you select **Last Name** in the **Search By** drop-down list.
   - In the **Group** field, the options are **Any** and the name of each group configured on Avaya one-X® Client Enablement Services.
   - In the **Server** field, the options are:
     - **Any**
     - **Telephony**
     - **Voice Messaging**
     - **Conferencing**
     - **Presence**
   - In the **Application** field, the option is:
     - **1XP**
   - In the **Log on** field, the options are:
     - **Either**
     - **Logged On**
     - **Logged Off**

Related topics:

Avaya one-X Client Enablement Services users configuration on page 102

Users field descriptions on page 120

Modifying provisioned users

Procedure

1. Select the **Users** tab.
2. From the left navigation pane, select **Provisioned Users**.
3. On the Provisioned Users page, search for the provisioned users to whom you want to add or modify resources, and click **Search** to display a list of those users.
4. Search by Any, Pattern, Group, Server, or Application, and click **Search** to display a list of users.
5. Click the **User Id** of the user you want to modify to display the View User page for that user.
6. To update an existing resource, click **Update** for that resource.
7. On the resource page, enter the appropriate information and click **Save**.

   For more information on the fields, see Users field descriptions on page 120.
8. Click **Delete** to delete a resource from the user.
9. After adding or updating the required resources, click **Finished** to return to the list of unprovisioned users.
10. On the Provisioned Users page, click the **User Id** of the user again.
11. On the View User page, click **Disable** to change the state of the user to disabled. The system displays the message: `User has been disabled`.
12. Click **Enabled**. The system displays the message: `User has been enabled`.
13. Click **Finished** to go back to the Provisioned Users page.

Related topics:

Avaya one-X Client Enablement Services users configuration on page 102
Users field descriptions on page 120

Modifying provisioned user groups

Procedure

1. Select the **Users** tab.
2. From the left pane, select **Provisioned Users**.

3. On the Provisioned Users page, search for the provisioned users to whom you want to add or modify resources and click **Search** to display a list of those users.
4. Search by Any, Pattern, Group, Server, or Application and click **Search** to display a list of users.
5. Click the **User Id** of the user you want to modify to display the View User page for that user.
6. To update the group of the user, in the **Group** section of the page, click **Update**.
7. At the Update Provisioned User Group Profile page, select a Group profile and click **Save**.
8. Click **Reset** to restore the fields to the last saved page or the default values if this is a new object.
9. Click **Cancel** to exit the page without making any changes.

Related topics:

Avaya one-X Client Enablement Services users configuration on page 102

Users field descriptions on page 120

Deleting provisioned users

Procedure

1. Select the **Users** tab.
2. From the left pane, select **Provisioned Users**.
3. On the Provisioned Users page, search for the user you want to delete.
4. Search by Any, Pattern, Group, Server, or Application and click **Search**.
5. Click the **User Id** of the user you want to delete.
   The system displays the View User page for the user.
6. Click **Disable** to change the user state.

   Note:

   To delete a user, you must disable the user first.
7. Click **Delete** to delete the user.

   Note:

   When you delete a user, all resources of that user such as telephone extension, voice mail account, and conference account are automatically deleted. However, deleting a user from Avaya one-X® Client Enablement Services does not delete them from the Enterprise Directory.

Related topics:

Avaya one-X Client Enablement Services users configuration on page 102
Users field descriptions on page 120

Enabling or disabling a user account

About this task

You can enable or disable a user account using the Client Enablement Services administration application. Only after you enable a user account in the administration application, the user can use all client application functionalities. The user resources should also be configured properly for the user before the user uses the client application.

You must disable a user account:

- When you assign or modify a telephony or mobile telephony resource to a user account.
- When you delete a user account.
- When you have to restrict a user login.

You must kill all active user sessions before disabling a user account.

Enabling the user account also sets the ONE-X mappings on Communication Manager for that user. Disabling the user account removes the ONE-X mappings on Communication Manager. If you want to completely remove the user account and release the license, you must delete the user account after you disable the user account.

Procedure

1. Select the **Users** tab.
2. From the left navigation pane, select **Provisioned Users**.
3. Search for and select the user whom you want to enable or disable.
4. On the View User page, perform one of the following:
   - Click **Enable** if the current state is **Disabled**.

     The system displays the message: `User has been enabled`.
   - Click **Disable** if the current state is **Enabled**.

     The system displays the message: `User has been disabled`.

Logging off and Killing user sessions

About this task

A session is created when the user logs in the user account using any Client Enablement Services client application. The **Sessions** section on the View User page displays the **Login Time** and **Session Type** of the current session.

As an administrator, you can log off the current session of a user in the client application or you can kill all sessions of the user.

✱ **Note:**

If you log in the administration application as an Auditor, you must not log off the user from an active session or kill the active sessions.

Procedure

1. Select the **Users** tab.
2. From the left pane, select **Provisioned Users**.
3. Search for and select the user whose session you want to end.

   You can log off the user session or kill the sessions.
4. In the **Sessions** section, you can:
   - click **Logoff Session** to log off the user from the current session.
   - click **Kill All Sessions** to kill all sessions of the user.

   The **Session Type** is displayed as **Portal** when the user is logged in the Avaya one-X® Communicator client or displayed as **Mobile** when the user is logged in the Avaya one-X® Mobile client.
5. Click **Finished**.

Related topics:

Users field descriptions on page 120

Checklist for assigning resources to a user

If you are installing either Avaya one-X® Communicator, or Avaya one-X® Mobile, or both, assign the following resources to a user in the Client Enablement Services administration application:

User resource	Avaya one-X® Mobile client	Avaya one-X® Communicator client with Client Enablement Services integration
Telephony resource	Yes This is a mandatory resource. This resource is required for all telephony features.	Yes This is a mandatory resource. This resource is required for all telephony features.
Mobile Telephony resource	Yes This is a mandatory resource. This resource is required for all mobile telephony features. If you do not assign this resource, users cannot log in to the Avaya one-X® Mobile client application.	Yes This is not a mandatory resource, but this resource is required for functionalities such as Block all calls.
Voice Messaging resource	Yes This is a mandatory resource. This resource is required for all features related to voice mails.	Yes This is a mandatory resource. This resource is required for all features related to voice mails.
Conferencing resource	No	Yes This is not a mandatory resource, but this resource is required for conferencing features such as bridge conferencing.
Presence resource	Yes This is not a mandatory resource, but this resource is required to view presence details of other users such as presence status (online, offline, busy), status message.	Yes This is not a mandatory resource. Avaya one-X® Communicator connects directly to the Presence server for presence features. However, when you assign a presence resource to an Avaya one-X® Communicator user, any presence update you make on one of the client application is reflected on the other.
Personal Contacts resource	No	Yes This is a mandatory resource. This resource is required for personal contacts synchronization of

User resource	Avaya one-X® Mobile client	Avaya one-X® Communicator client with Client Enablement Services integration
		the Client Enablement Services database and Avaya one-X® Communicator. Do not configure the personal contact resource for users using Avaya one-X® Communicator Release 6.1 SP3. Hence, for such users, this is not a mandatory resource.

Assigning a Telephony resource to a user

Before you begin

Do not add, delete, or modify a telephony resource while the user is logged in to the Avaya one-X® Mobile client application. This might cause an account setup failure of the client application at the next user login. To avoid this account setup failure, you must first disable the user account and then add, delete, or modify a telephony resource.

About this task

You must assign a telephony resource to a user after you provision the user.

You can also use the Administration Command Line Interface to assign a telephony resource to a user on Avaya one-X® Client Enablement Services.

To assign a telephony resource to a user using the CLI, see Create a user resource on page 201.

Procedure

1. In the Administration application, click the **Users** tab.
2. From the left pane, select **Provisioned Users**.
3. Search for and select the user to whom you want to assign the resource.
4. In the **Telephony** group box, click **Add**.
5. Complete the following fields:
    a. From the **Server** drop-down list, select the handle of the Communication Manager.

       This is a mandatory field.

b. In the **Display Name** field, type a descriptive name for this resource which users will see in the Client Enablement Services.

   This is a mandatory field.

c. In the **Display Address** field, type the text to display in the Client Enablement Services for this extension.

d. In the **Extension** field, type the extension assigned to the user.

   This is a mandatory field.

   Note that users cannot update the extension using the client application.

   Note:

   - The extension whether H.323 or SIP must exist on the Communication Manager before you assign it to the user on Client Enablement Services.
   - You must not configure the same desk phone extension for two or more users in one Client Enablement Services server.
   - You must not configure a desk phone extension on a Client Enablement Services server that is already configured on another Client Enablement Services server. This causes problems with call routing and impacts client application features such as multiple ring phone destinations, block all calls, allow only VIP calls.

   To identify if a desk phone extension is already configured on the Client Enablement Services server, go to the Provisioned Users search page, you can select **Extension** in the **Search By** drop-down list, enter the desk phone extension you want to configure in the **Pattern** field, and click **Search**. If the system displays a user is already configured with the same desk phone extension number, do not configure any other user with this desk phone extension number on the same or any other Client Enablement Services server.

e. Select a destination routing from the **Destination Routing** drop-down list. The system routes the incoming calls to number based on the Destination routing configured for the user.

6. Click **OK** to save the field values.
7. Click **Finished**.
8. Click **Delete** to delete this resource.

   Note:

   You must disable the user before deleting a resource assigned to the user.

Assigning a Mobile Telephony resource to a user

Before you begin

You must assign a telephony resource to a user before you assign a mobile telephony resource to a user.

Do not add, delete, or modify a mobile telephony resource while the user is logged in to the Avaya one-X® Mobile client application. This might cause an account setup failure of the client application at the next user login. To avoid this account setup failure, you must first disable the user account and then add, delete, or modify a mobile telephony resource.

About this task

If you do not assign a mobile telephony resource to a user, the user cannot log in to the Avaya one-X® Mobile client application.

When you assign this resource to a user, Client Enablement Services enables the extension of the user on Communication Manager for Also Ring, Call back, Call logging, Block all calls, and VIP calling features.

For Client Enablement Services deployments with both Avaya one-X® Communicator and Avaya one-X® Mobile client applications, following features can be controlled using either client application:

- Block all calls
- VIP calling
- Call logging
- Also ring
- Call back

Procedure

1. In the Administration application, select the **Users** tab.
2. From the left pane, select **Provisioned Users**.
3. Search for and select the user to whom you want to assign the mobile telephony resource.
4. In the **Mobile Telephony** group box, click **Add**.

   You can assign only one mobile telephony resource to a user.
5. On the Add Resource page, complete the following fields:
   a. The **Mobile SMS Address** field displays the SMS address configured by the user in the Avaya one-X® Mobile client application.

      You cannot modify this field. The field value changes whenever the user changes the SMS address in the client application.

All SMS messages sent by Client Enablement Services are sent to this SMS address.

b. Select a routing configuration from the **Mobile Routing** drop-down list. The incoming calls are routed to a mobile number based on the Mobile routing configured for the user.
c. Select a routing configuration from the **Ring-also Routing** drop-down list. The system routes the incoming calls to a number other than the mobile number based on the Ring-also routing configured for the user.
d. Select a routing configuration from the **Callback Routing** drop-down list. The system routes the calls to a number specified by the user for callback based on the routing configuration selected for callback.
e. In the **Display Name** field, enter a descriptive name for this telephony resource which users see in Client Enablement Services.

   This is a mandatory field.
f. In the **Display Address** field, enter the text to display in Client Enablement Services for this extension.
g. In the **Mobile Number** field, enter the mobile number of the user.

   Note:

   - You must not configure the same mobile number for two or more users in one Client Enablement Services server.
   - End users are also not allowed to update their mobile numbers in the client application to a number that is already configured for another user on the Client Enablement Services server.
   - The mobile number you enter must be routable as per the ARS table configured in Communication Manager.
h. In the **Mobile Manufacturer** field, enter the manufacturer of the mobile.
i. Select the **Lost or Stolen Device** check box if the mobile gets lost or stolen. When you select this check box, the Client Enablement Services server notifies the Avaya one-X® Mobile client application to remove all locally stored data, such as downloaded voice mail, clear the account information, and force the user to re-login in order to access Avaya one-X® Mobile. The user is then unable to use Avaya one-X® Mobile on any mobile device until the you clear this check box.
j. In the **Mobile Model** field, enter the model of the mobile.

6. Click **OK** or **Save** to save your changes.
7. Click **Delete** to delete this resource.

   Note:

   You must disable the user before deleting a resource assigned to the user.
8. Click **Reset** to display the settings from the start of this session.

9. Click **Cancel** to cancel the changes you made.

Result

When you assign a mobile telephony resource to a user and the user logs in the client application, the mobile number of the user is saved as an ONE-X mapping on the STATION TO OFF-PBX TELEPHONE MAPPING screen on Communication Manager. To verify the Client Enablement Services control on the extension of the user on Communication Manager, use the command **`status station < extension number>`**. The **one-X Server Status** field displays the status as either: **Trigger**, **Normal**, **No-ring**, **Voicemail**. However, when you delete this resource, the control is withdrawn, and the status is set to **N/A**.

Related topics:

System profile and Group profile field descriptions on page 92
Assigning a Voice Messaging resource to a user on page 115
Notification on page 151
Configuring the Feature-Related System Parameter screen on page 249
Extension to Cellular and Client Enablement Services on page 258
Client Enablement Services user mapping is not in sync with Communication Manager on page 311

Assigning a Voice Messaging resource to a user

About this task

Voice messaging is a mandatory resource, and you must assign this resource to all users. After you add the Voice Messaging resource, users can connect to their mailbox on the Messaging server

You can also use the Administration Command Line Interface to assign resources to users on Client Enablement Services.

To assign a voice messaging resource using CLI, see Create a user resource on page 201.

Procedure

1. Select the **Users** tab.
2. From the left pane, select **Provisioned Users**.
3. Search for and select the user to whom you want to assign the resource.
4. In the **Voice Messaging** group box, click **Add**.
5. Complete the following fields:
   a. From the **Server** drop-down list, select the handle of the messaging server.
   b. In the **Primary voicemail number** field, enter the voice mail number of the user using which the user can access voice mails.

c. In the **Display Name** field, enter a descriptive name for this resource which users see in the Client Enablement Services.

   This is a mandatory field.

d. In the **Display Address** field, enter text to display in Client Enablement Services for this mailbox.

e. In the **Mailbox** field, enter the mailbox assigned to the user.

f. In the **Password** field, enter the password only if you know the password of the mailbox of the user. If you do not know the password, do not enter any value in this field.

   You must enter the mailbox number of the user, but you can leave the password field blank. User can enter the password when logging in through the client application.

g. In the **Confirm** field, enter the password only if you know the password of the mailbox of the user. If you do not know the password, do not enter any value in this field.

h. In the **Web Subscriber Options URL** field, enter the URL of Web Subscriber Options service of the Modular Messaging server from where users can make changes to their voice mailbox settings such as when the message waiting indicator comes on.

   Enter the URL in the **Web Subscriber Options URL** field, only if you are using a Modular Messaging server as the messaging server. The **Web Subscriber Options URL** field is not available if the voice messaging server is either Avaya Aura® Messaging or Communication Manager Messaging.

i. From the **SMS notification** drop-down list, select **All**, **None**, or **Priority**. If SMS Notification is set to **None**, user does not receive any notification of a new voice mail. If SMS Notification is set to **All**, user receives notifications for all new voice mails. If SMS Notification is set to **Priority**, user receives notifications of voice mails from contacts marked as priority.

6. Click **OK** to save the field values.

7. After making changes to all other user resources, click **Finished**.

8. Click **Delete** to delete this resource.

   Note:

   You must disable the user account before deleting a resource assigned to the user.

Related topics:

System profile and Group profile field descriptions on page 92
Assigning a Mobile Telephony resource to a user on page 113
Notification on page 151

Assigning a Conferencing resource to a user

About this task

You must assign a conferencing resource for all Avaya one-X® Communicator users who need to use the conferencing feature in Avaya one-X® Client Enablement Services. Users do not have permissions to add or delete conferencing resources in their Client Enablement Services settings. Users can only update an existing conferencing resource.

Note:

To enable users to have access to the conferencing feature, you must enable the user in Conferencing as well.

You can also use the Administration Command Line Interface to assign resources to users on Client Enablement Services.

To assign a conferencing resource to a user using CLI, see Create a user resource on page 201.

Procedure

1. Select the **Users** tab.
2. From the left pane, select **Provisioned Users**.
3. Search for and select the user to whom you want to assign the resource.
4. In the **Conferencing** group box, click **Update**.
5. Complete the following fields:
    a. From the **Server** drop-down list, select the handle of the Conferencing server.
    b. In the **Display Name** field, enter a descriptive name for the resource that users see in Client Enablement Services.

       This is a mandatory field.
    c. In the **Display Address** field, enter text to display in Client Enablement Services for this conferencing account.
    d. In the **Moderator Code** field, enter the host code assigned to the account.
    e. In the **Participant Code** field, enter the participant code assigned to the account.
    f. In the **PIN Code** field, enter the unique PIN code assigned to the account.

       Each user must have a unique PIN Code. If duplicate PIN Codes are assigned, the users with the duplicate PIN codes are not able to participate in bridge conferences if another user with the same PIN code is already participating in a conference.
    g. In the **Bridge Number** field, enter the telephone number that the user dials to log in to the bridge.
    h. In the **Bridge Number Backup** field, enter the secondary telephone number that the user can dial to log in to the bridge.

6. Click **Save** to save your changes.
7. Click **Reset** to reset the page settings.
8. After making changes to other resource, click **Finished**.

Assigning a Presence resource to a user

About this task

You must assign a presence resource to all users who want to publish their presence state to watchers on Avaya one-X® Client Enablement Services.

You can also use the Administration Command Line Interface to assign resources to users on Client Enablement Services.

To assign a presence resource to a user, see Create a user resource on page 201.

Procedure

1. In the Administration application, select the **Users** tab.
2. From the left pane, select **Provisioned Users**.
3. Search for and select the user to whom you want to assign the resource.
4. In the **Presence Information** group box, click **Update**.
5. Complete the following fields:
    a. From the **Server** drop-down list, select the handle of the Avaya Aura® Presence Services server.
    b. In the **Display Name** field, enter a descriptive name for the resource that users see in Client Enablement Services.
       This is a mandatory field.
    c. In the **Display Address** field, enter text to display in Client Enablement Services for this presence account.
6. Click **Save** to assign the server to the user.
7. After making changes to other user resources, click **Finished**.
8. Click **Delete** to delete this resource.

   You must disable the user before deleting a resource assigned to the user.

Assigning a Personal contact resource to a user

About this task

Client Enablement Services manages Avaya one-X® Communicator contacts when the Avaya one-X® Communicator client application is integrated with Client Enablement Services. When you add a contact in Avaya one-X® Communicator, it sends a request to the Client Enablement Services server to add this contact for the Avaya one-X® Communicator user in the Client Enablement Services database.

Client Enablement Services uses the Personal Contact adapter and Personal Contact service to understand this request and store this information in the database. Therefore, you must add a Personal Contact resource to a user who is using the Avaya one-X® Communicator client application.

Note:

Do not assign a personal contact resource to users using Avaya one-X® Communicator Release 6.1 SP3.

Procedure

1. In the Administration application, select the **Users** tab.
2. From the left pane, select **Provisioned Users**.
3. Search for and select the user to whom you want to assign the resource.
4. In the **Personal Contacts** group box, click **Add**.
5. On the Add Resource page, complete the following fields:

   The **Server** field displays the personal contact server configured for the user who is using the Avaya one-X® Communicator client application. The system displays the field value as **PersonalContactProviderDefault**. You cannot change this field value.

   a. In the **Display Name** field, type a descriptive name for the resource.

      This is a mandatory field.

   b. In the **Display Address** field, type the text to display in the client application for the Personal Contact resource.

   c. In the **Email Address** field, type the e-mail address of the user.

6. Click **OK** or **Save** to save your changes.
7. Click **Delete** to delete this resource.

   You must disable the user before deleting a resource assigned to the user.

8. Click **Reset** to display the settings from the start of this session.
9. Click **Cancel** to cancel the changes you made.

Users field descriptions

Name	Description
User ID	The unique identifier assigned to the provisioned user by the administrator.
First Name	The first name of the provisioned user.
Last Name	The last name of the provisioned user.
Nick Name	The familiar or nickname used to identify provisioned user.
State	The current state of the user: **Enabled** or **Disabled**.
Group	The name of the group profile, if any, to which the user is assigned. Click **Update** to edit the Group profile.
Sessions	
Login Time	The log-in date and time of the session to which the user is logged in. For example, Tues Mar 13 17:05:01 EDT 2007.
Session Type	The type of session to which the user is logged in. For example, Mobile.
Logoff Session	Select this option to log the user off the current session.
Kill All Sessions	Select this option to terminate all active sessions for the user.
Telephony	The **Telephony** fields pertain to the Communication Manager used for Telephony services. Avaya one-X® Client Enablement Services supports one Telephony resource per user.
Server	The name of the Communication Manager to which the user is connected for Telecommuter, Mobility, and other Telephony services.
Display Name	The name assigned to the phone extension used for Telephony services.
Display Address	The display address of the phone extension used for Telephony services.

Name	Description
Extension	The desk phone extension used for Telephony services.
Destination Routing	The system routes the incoming calls to number based on the Destination routing configured for the user.
Property	The Value and Source assigned to the Send DTMF for calls property. This is read-only field because **Value** and **Source** are inherited from either the System profile or the Group profile assigned to the user.
Mobile Telephony	The **Mobile Telephony** fields pertain to the integration between the user enterprise telephony with the mobile device of the user.
Mobile Routing	The incoming calls are routed to a mobile number based on the Mobile routing configured for the user.
Ring-also Routing	The system routes the incoming calls to a number other than the mobile number based on the Ring-also routing configured for the user.
Callback Routing	The system routes the calls to a number specified by the user for callback based on the routing configuration selected for callback. **Note:** When the user makes a callback call using the desk phone as the originating entity, then for: • H.323. The desk phone directly calls the destination number. • SIP. User needs to first pick up the desk phone receiver, and only then the destination number is called.
Display Name	The name assigned to the mobile device used for Mobile Telephony services.
Display Address	The address assigned to the mobile device used for Mobile Telephony services.
Mobile Number	The mobile number of the user.
Mobile Manufacturer	The manufacturer of the mobile device.

Name	Description
Lost or Stolen Device	Select this option to indicate if the mobile device of the user is lost or stolen. When you select this check box, the Client Enablement Services server notifies the Avaya one-X® Mobile application to remove all locally stored data such as downloaded voice mail; to clear the account information such as user name, server; and to force the user to re-login to access the Avaya one-X® Mobile application. The user cannot use the Avaya one-X® Mobile application on any mobile device till you clear this check box.
Mobile Model	The model of the mobile device.
Mobile SMS Address	This field displays the SMS address configured by the user in the Avaya one-X® Mobile client application. This field cannot be modified by administrators. The field value changes whenever the user changes the SMS address in the client application. All SMS messages sent by Client Enablement Services are sent to this SMS address.
Property	The **Value** and **Source** assigned to the DTMF detection for inbound calls, Extension Contact Logging, and DTMF detection for callback properties. These are read-only fields because **Value** and **Source** are inherited from either the System profile or Group profile assigned to the user.
Voice Messaging	The **Voice Messaging** fields pertain to the messaging server used for Voice Messaging services. Client Enablement Services supports multiple messaging servers per user.
Server	The name of the messaging server to which the user account is configured for Voice Messaging services.
Primary voice mail number	The primary voice mail number of the mailbox of the user.
Display Name	The name assigned to the mailbox used for Voice Messaging services.
Display Address	The display address of the mailbox used for Voice Messaging services.

Name	Description
Mailbox	The identifier assigned to the mailbox used for Voice Messaging services.
Password	The password assigned to the user to gain access to Voice Messaging services.
Confirm	Confirm the password.
Web Subscriber Options URL	URL of the Web Subscriber Options service of the Modular Messaging server from where users can make changes to their voice mailbox settings such as when the message waiting indicator comes on. Enter the URL in the **Web Subscriber Options URL** field, only if you are using a Modular Messaging server as the messaging server.
SMS notification	• If SMS Notification is set to **None**, user do not receive any notification of a new voice mail. • If SMS Notification is set to **All**, user receives notifications for all new voice mails. • If SMS Notification is set to **Priority**, user receives notifications of voice mails from contacts marked as priority.
Property	The **Value** and **Source** assigned to Maximum Voice Messages, Forward Voice Messages, and Save Voice Messages properties. These are read-only fields because **Value** and **Source** are inherited from either the System profile or Group profile assigned to the user.
Conferencing	The **Conferencing** fields pertain to the Conferencing server used for Conferencing services. Client Enablement Services installs one Conferencing resource per user. You can modify this resource but you cannot delete it.
Server	The name of the Conferencing server to which the user is connected for Conferencing services.
Allow Call Me	If selected, user can receive an incoming call from the bridge conference. This enables the

Name	Description
	user to join in the conference automatically without requiring manual inputs of host/ participant code. **Note:** This feature works only when the bridge and the conference are configured to allow out-dialing.
Display Name	The name assigned to the phone extension used for Conferencing services.
Display Address	The display address of the phone extension used for Conferencing services.
Pin Code	The user password for the Conferencing server. This is an optional field in most Conferencing servers. You should enter this value only if your Conferencing server requires a password.
Moderator Code	The code used by the user who moderates the conference. The user must enter this code to make the conference available to the other attendees.
Participant Code	The code used by the users who attend the conference. The moderator must enter the moderator code to make the conference available to these users.
Bridge Number	The phone number used for the conference call. All attendees dial this number to access the conference.
Bridge Number Backup	The backup phone number used for the conference call when the original bridge number is unavailable.
Property	Conference Contact Logging
Presence Information	The **Presence Information** fields pertain to the Presence server used for accessing the presence details of a user.
Server	Handle of the Presence server configured on the Client Enablement Services server.
Display Name	A descriptive name for the presence resource that users see in the client application.

Name	Description
Display Address	The text to display in the client application for the presence resource.
Personal Contact	The **Personal Contact** fields pertain to the Exchange server used for accessing the contacts of a user.
Server	Handle of the Exchange server on which the user has an outlook account.
Display Name	A descriptive name for the resource that users see in the client application.
Display Address	The text to display in the client application for the Personal Contact resource.
Email Address	E-mail address of the user configured on the Exchange server.

Related topics:

System Profile on page 87
Displaying the System Profile on page 88
Modifying the System profile on page 88
Group Profiles page on page 89
Adding group profiles on page 90
Listing group profiles on page 91
Modifying group profiles on page 91
Prototype Users on page 96
Adding Prototype users on page 96
Listing Prototype users on page 97
Modifying Prototype Users on page 101
Avaya one-X Client Enablement Services users configuration on page 102
Provisioning an unprovisioned user on page 103
Listing provisioned users on page 104
Modifying provisioned users on page 106
Modifying provisioned user groups on page 106
Deleting provisioned users on page 107
Logging off and Killing user sessions on page 109

Chapter 5: Scheduler administration

Overview

Using Avaya one-X® Client Enablement Services Scheduler, you can automate the execution of certain tasks by scheduling the processes that control those tasks. You can also perform the following tasks on a daily, weekly, or monthly schedule at a specified time of day.

- Scheduling Contact Log Cleanup on page 127
- Scheduling Database Backup on page 129
- Scheduling Enterprise Directory Synchronization on page 130
- Scheduling Voice Messaging Synchronization on page 132
- Scheduling Statistics Cleanup on page 133

You should schedule these tasks at different times of the day or week, so that all tasks are not scheduled at the same time. You should avoid scheduling these tasks when the system back up is scheduled.

You can view the log activity of any task through the Trace log. For more information, see Logging on page 159.

Note:

If you are an **Auditor**, the **Scheduler** tab is not available.

Scheduling Contact Log Cleanup

About this task

The Contact Log Cleanup option trims the number of Contact Log records that Avaya one-X® Client Enablement Services stores for each user. The records get trimmed depending on the values set in the following fields:

- **Users** > **System Profile** > **Maximum number of history records**: All records exceeding the number set in this field gets deleted. The oldest record is deleted first.
- **Users** > **System Profile** > **Maximum days to keep history**: All records older than the value set in this field gets deleted.

Therefore, the contact log may appear empty if the last call log is older than the value set in **Maximum days to keep history**.

Schedule Contact Log Cleanup based on the total amount of storage available on your system and the number or records you want to save for each user.

Procedure

1. Select the **Scheduler** tab.

   Note:

   If you are an **Auditor**, the **Scheduler** tab is not available.

2. From the left pane, select **Contact Log Cleanup**.
3. On the Contact Log Cleanup Settings page, select the **Enabled** check box.
4. In the **Cleanup Schedule Mode** section, set the schedule parameters.
   - **Daily**. Runs the task every day at the specified time.
   - **Weekly**. Runs the task every week on the specified day of the week.
   - **Monthly**. Runs the task each month on the specified day of the month.
5. In the **Day** field, set the run parameters of the schedule.
   - If you select **Daily** in the **Cleanup Schedule Mode** section, this field is disabled by default.
   - If you select **Weekly** in the **Cleanup Schedule Mode** section, select the day of the week to run the task.
   - If you select **Monthly** in the **Cleanup Schedule Mode** section, select the day of the month (0-31) on which to run the task.
6. In the **Hour** field, select the hour of the day (0-23) in which to run the task.
7. In the **Minute** field, select the minute (0-59) of the hour in which to run the task.
8. Click **Run Now** to run the task immediately to incorporate these changes.
9. Click **Save** to save the current settings on this page.
10. Click **Reset**. This restores the settings to the last saved page. If this is a new object, it restores the settings to the default values.

Related topics:

Scheduler field descriptions on page 134

Scheduling Database Backup

About this task

Use the schedule database backup to take regular backups of the Client Enablement Services database to a predefined directory location. The system performs the scheduled database backup at this location only.

For remote backups, you can use the template backup feature. You should use the System Platform backup and restore procedure to back up and restore the Client Enablement Services template. For more information on template backup and restore, see Backup and restore overview on page 231.

You must schedule database backup when the system is not in use because it takes the Client Enablement Services database off line.

The database file that is backed up using the scheduler is `ACPDB.0.dbinst.NODE0000.CATN0000.xxxxxxxxxxxxxx.xxx`. In this file, xxx is the time stamp.

Procedure

1. Select the **Scheduler** tab.

   Note:

   If you are an **Auditor**, the **Scheduler** tab is not available.
2. From the left pane, select **Database Backup**.
3. Select the **Enabled** field.
4. In the **Full Backup Schedule Mode** section, set the schedule parameters:
   - **Daily**. Runs the task every day at the specified time
   - **Weekly**. Runs the task every week on the specified day of the week
   - **Monthly**. Runs the task each month on the specified day of the month
5. In the **Day** field, specify the run parameters of the schedule:
   - If you select **Daily** in the **Full Backup Schedule Mode** section, this field is disabled by default.
   - If you select **Weekly** in the **Full Backup Schedule Mode** section, select the day of the week to run the task.
   - If you select **Monthly** in the **Full Backup Schedule Mode** section, select the day of the month (0-31) on which to run the task.
6. In the **Hour** field, select the hour of the day (0-23) in which to run the task.
7. In the **Minute** field, select the minute (0-59) of the hour in which to run the task.

8. The **Backup File to Location** field is set to `/opt/avaya/1xp/dbbackup`. This is the path of the directory where the database backup is stored and this field is not editable.
9. Click **Run Now** to run the task immediately to incorporate these changes.

   To track the status of this operation, refresh the page.
10. Click **Save** to save the current settings on this page.
11. Click **Reset**. This restores the settings to the last saved page. If this is a new object, it restores the settings to the default values.

Related topics:

Scheduler field descriptions on page 134

Backing up and restoring the database on page 240

Managing disk space on the Avaya one-X Client Enablement Services template on page 243

Scheduling Enterprise Directory Synchronization

About this task

You must synchronize the users added to the Avaya one-X® Client Enablement Services database with the Enterprise Directory database. Enterprise Directory Synchronization is the process of synchronizing user provisioning and contact data in the Client Enablement Services database with user data in the Enterprise Directory.

During this process, Client Enablement Services compares the records in its database with the records in Enterprise Directory. If there is a change in Enterprise Directory, Client Enablement Services makes the corresponding change in its database. The records that Client Enablement Services compares include the unprovisioned user list, enterprise contact information, and Client Enablement Services user information. Other LDAP Enterprise Directories are also supported in this process.

Schedule Enterprise Directory Synchronization based on the number of users added to the Client Enablement Services database over a specified period of time. A full synchronization includes all of the data records in the database. An incremental synchronization includes all the data records since the last full synchronization.

Procedure

1. Select the **Scheduler** tab.

   Note:

   If you are an **Auditor**, the **Scheduler** tab is not available.
2. From the left pane, select **Enterprise Directory Synchronization**.

3. Select **Enabled**.
4. In the **Synchronization Schedule Mode** section, select the schedule parameters.
    - **Daily**. To run a full synchronization every day at the specified time.
    - **Weekly**. To run a full synchronization every week on the specified day of the week.
5. In **Daily** mode:
    - **Day of the Week**. In this field, specify the day (Sunday-Saturday) to run a full synchronization of the task. On all other days, the system runs incremental synchronization.
    - **Hour**. In this field, select the hour of the day (0-23) in which to run the task.
    - **Minute**. In this field, select the minute (0-59) of the hour in which to run the task.

    If you do not select any of these, the system performs only incremental synchronizations.
6. In **Weekly** mode:
    - **Week of the Month**. In this field, specify the weeks (1st-4th) to run a full synchronization of the task. On all other days, the system runs incremental synchronization.
    - **Day of the Week**. In this field, specify the day to run the task.
    - **Hour**. In this field, select the hour of the day (0-23) in which to run the task.
    - **Minute**. In this field, select the minute (0-59) of the hour in which to run the task.

    If you do not select any of these, the system performs only incremental synchronizations.
7. Click **Run Full Sync Now** for full synchronization or click **Run Incremental Sync Now** for an incremental synchronization to run immediately and incorporate these changes.

    To track the status of this operation, refresh the page.

    Note:

    You must run a full enterprise directory synchronization when you delete one or more users from the enterprise directory. Only then, the users get deleted from the Client Enablement Services server.
8. Click **Save** to save the current settings on this page.
9. Click **Reset**. This restores the settings to the last saved page. If this is a new object, it restores the settings to the default values.

Related topics:

[Scheduler field descriptions](#) on page 134
[Modifying LDAP attribute mappings](#) on page 141
[Modifying the LDAP filter for importing selected users](#) on page 142

Scheduling Voice Messaging Synchronization

About this task

Using the Voice Messaging option, you can gain access to the user details on the messaging server and match the user details with the Avaya one-X® Client Enablement Services Contact Service. When a match is found for either the telephone, or the extension, or the e-mail handle, Client Enablement Services associates a new voice mail handle with the contact.

Schedule Voice Messaging based on the number of contacts added to Client Enablement Services over a specified period of time.

Note:

Running this operation can impact system performance. Do not run this operation with a high volume of users actively using Client Enablement Services. Run this operation during off hours.

Procedure

1. Select the **Scheduler** tab.

   Note:

   If you are an **Auditor**, the **Scheduler** tab is not available.

2. From the left pane, select **Voice Messaging Synchronization**.
3. Select the **Enabled** field.
4. In the **Synchronization Schedule Mode** section, set the schedule parameters:
   - **Daily**. Runs the task every day at the specified time.
   - **Weekly**. Runs the task every week on the specified day of the week.
   - **Monthly**. Runs the task every month on the specified day of the month.
5. In the **Day** field, specify the run parameters of the schedule:
   - If you select **Daily** in the **Synchronization Schedule Mode** section, this field is disabled by default.
   - If you select **Weekly** in the **Synchronization Schedule Mode** section, select the day of the week to run the task.

- If you select **Monthly** in the **Synchronization Schedule Mode** section, select the day of the month (0-31) on which to run the task.

6. In the **Hour** field, select the hour of the day (0-23) in which to run the task.
7. In the **Minute** field, select the minute (0-59) of the hour in which to run the task.
8. Click **Run Now** to run the task immediately to incorporate these changes.
9. Click **Save** to save the current settings on this page.
10. Click **Reset**. This restores the settings to the last saved page. If this is a new object, it restores the settings to the default values.

Related topics:

Scheduler field descriptions on page 134

Scheduling Statistics Cleanup

About this task

The Statistics Cleanup option deletes statistics records in the Avaya one-X® Client Enablement Services database if their collection time is older than the configured retention time. This helps control the number of retained statistics records in the database.

There are two Scheduler tasks for cleaning up statistics, one for each type of statistics, Usage statistics and Performance statistics. Statistics retention time is specified on the **System** tab for statistics. Refer to Configuring statistics on page 159.

Procedure

1. Select the **Scheduler** tab.

   Note:

   If you are an **Auditor**, the **Scheduler** tab is not available.

2. In the left pane, select **Statistics Cleanup**.
3. In the **Usage Statistics Cleanup Settings** section, select **Enabled**.
4. In the **Usage Cleanup Mode** section, set the schedule parameters:
   - **Daily**. Runs the task every day at the specified time.
   - **Weekly**. Runs the task every week on the specified day of the week.
   - **Monthly**. Runs the task each month on the specified day of the month.
5. In the **Day** field, specify the run parameters of the schedule:

- If you select **Daily** in the **Usage Cleanup Mode** section, this field is disabled by default.
- If you select **Weekly** in the **Usage Cleanup Mode** section, select the day of the week to run the task.
- If you select **Monthly** in the **Usage Cleanup Mode** section, select the day of the month (0-31) on which to run the task.

6. In the **Hour** field, select the hour of the day (0-23) in which to run the task.
7. In the **Minute** field, select the minute (0-59) of the hour in which to run the task.
8. Click **Run Now** to run the task immediately to incorporate these changes.

   Note:

   Some tasks, such as Database backup, affect the operation of the system.
9. In the **Performance Statistics Cleanup Settings** section, select **Enabled**.
10. Set up and schedule using the same procedures as **Usage Statistics Cleanup Settings** above.
11. Click **Save** to save the current settings on this page.
12. Click **Reset**. This restores the settings to the last saved page. If this is a new object, it restores the settings to the default values.

Related topics:

Scheduler field descriptions on page 134
Statistics field descriptions on page 170

Scheduler field descriptions

Name	Description
Enabled	If selected, enables scheduling of cleanup or synchronization settings. **Note:** Enable the **Statistics Cleanup** settings for **Usage Statistics** and **Performance Statistics** when you select the **Enable Collection** check box for **Usage Statistics** and **Performance Statistics** on the **System** tab.

Name	Description
Schedule Mode	Lists the various scheduling options for the specified task. • For Enterprise Directory Servers, pertains to Full and Incremental synchronizations. • For Statistics Cleanup, pertains to Usage and Performance statistics.
Daily	Schedules the task to run every day at the specified time.
Weekly	Schedules the task to run every week on the specified day of the week.
Monthly	Schedules the task to run every month on the specified day of the month.
Week of the Month	Specifies the week of the month to run the task.
Day of the Week	Specifies the day of the week to run the task.
Day	For a **Daily** schedule, this field is disabled. For a **Weekly** schedule, specifies the day of the week on which to run the task. For a **Monthly** schedule, specifies the day of the month (1-31) on which to run the task.
Hour	For all schedule types, specifies the hour of the day (0-23) on which to run the task.
Minute	For all schedule types, specifies the minute of the specified hour (0-59) on which to run the task.
Backup File to Location	For database backup, specifies the path name of the directory where the backup file is to be stored. **Note:** The **Backup File To Location** field value is `/opt/avaya/1xp/dbbackup`. This field is not editable.
Run Now	Runs the task immediately to incorporate recent changes. This button allows the task to be run one time per change. **Note:** Some tasks, such as database backup and Directory Server Synchronization, affect the operation of the system.

Name	Description
Save	Saves the current settings on the page.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Task Status	The **Task Status** fields include the **Time**, **Task ID**, **Task Type**, and **Task Status** of the scheduling task. The **Task Status** fields display a list of previous schedule runs, which shows the history of this task. When you start a new task run, leave the Scheduler page, and return to display the status of the current run. The system no longer displays the previous runs. You must leave the Scheduler page to update the status of the run. At the end of the run, the system displays a success or failure message.

Chapter 6: System administration

General settings

When you enter an incorrect user name or password in the Avaya one-X® Client Enablement Services administration application login screen, the system displays an error message and provides you a link to send an e-mail to the system administrator. You can specify an e-mail address in the **Administrator Contact URL** field using which the user can contact the administrator for technical assistance.

Related topics:

Configuring general settings on page 137

General Settings field descriptions on page 162

Configuring general settings

Procedure

1. Click the **System** tab.
2. In the left pane, select **General**.
3. In the **Administrator Contact URL** field, enter an e-mail address to contact the system administrator.
   For the e-mail address, type `mailto:sysadmin@usa.com`.

   This address is displayed in the error messages that suggest the administrator to ask for assistance from the system administrator.
4. In the **Product ID** field, enter the ID of the product for which you need support.
5. The **Presence Domain Rule From** field specifies the domain of the Avaya one-X® Client Enablement Services system.

   The field value of this field is non configurable and set at the time of Client Enablement Services installation.
6. In the **Presence Domain Rule To** field, enter the domain of the Presence Services system.

Note:

Once you have configured the Presence Services system and it is working, you must not modify this field.

7. The **Application Server Version** field displays the version of Client Enablement Services.
8. The **Database Server Version** field specifies the version of the database server of Client Enablement Services.
9. Click **Save** to save the change.
10. Click **Reset** to display the settings from the start of this session.

Related topics:

General settings on page 137

General Settings field descriptions on page 162

Enterprise Directory domains

Avaya one-X$^{®}$ Client Enablement Services connects to the enterprise directory to search for users, security groups, and contacts. Users must exist in the enterprise directory before they can be provisioned as users on Client Enablement Services.

Client Enablement Services supports Active Directory configuration in either of these setup:

- single setup
- split domain setup

Except Active Directory, all other enterprise directories require the User domain and Resource domain to be on the same server.

- The User domain can contain users, security groups, and contacts. The users and security groups can be setup on single server or in split-server mode.
- The Resource domain contains security groups. Security groups are privilege-based groups set in the Active Directory. These groups are defined by their permissions on Client Enablement Services, such as Administrator, Auditor, or User. Active Directory is generally configured in split-server multi domain mode if its Resource domain is different from the User domain.
- Contact domains contain information about the contacts with which Client Enablement Services users communicate. Contact information includes details such as name, phone number, and address.

You can define only one User domain and one Resource domain at the time of installation. After installing Client Enablement Services, you cannot add, modify, or delete a User domain or Resource domain. If you want to make any changes to User domain or Resource domain, you have to re-install Client Enablement Services.

However, you can add a Contact domain and modify the names of existing Contact domains but you cannot change the type of a Contact domain. For example, if your enterprise acquires another company, you may want to access the contact information for the other company in a new Contact domain. If you want to add a Contact domain, it must be the same type as the User domain and Resource domain. For example, if you are using Active Directory for your user domain, then all the contact directories must be in Active Directory.

Note:

- You can add only Active Directory LDAP as the Contact Domain. You can add Active Directory LDAP as the Contact Domain only when the primary LDAP is also Active Directory.
- Client Enablement Services does not support integration with the Avaya Presence Services server if you are using Microsoft Active Directory Application Mode (ADAM) as the enterprise directory.

Related topics:

Listing Enterprise Directory domains on page 139
Adding the contact domains on page 140
Modifying Domains on page 140
Modifying LDAP attribute mappings on page 141
Modifying LDAP attribute mappings for a split domain topology on page 142
Modifying the LDAP filter for importing selected users on page 142
Enterprise Directory field descriptions on page 163

Listing Enterprise Directory domains

Procedure

1. Click the **System** tab.
2. In the left pane, select **Enterprise Directory** .
3. On the Enterprise Directory Domains page, click the name of a domain in the **Domain** field to display the View Enterprise Directory Domain page.

Adding the contact domains

About this task

Users can use this contact domain only to search contacts.

Procedure

1. Click the **System** tab.
2. In the left pane, select **Enterprise Directory**.

   The Enterprise Directory Domains page displays a list of the domains on the system.
3. Click **Add Contact Domain** to display the Add Enterprise Contact Domain page.

   > **Note:**
   >
   > You can add only Active Directory LDAP as the Contact Domain. You can add Active Directory LDAP as the Contact Domain only when the primary LDAP is also Active Directory.
4. Enter the appropriate information and click **OK** to add the domain.

   For more information on the fields, see Enterprise Directory field descriptions on page 163.
5. Click **Reset** to restore the settings to the last saved page or, if this is a new object, the default values.
6. Click **Cancel** to exit the page without making any changes.

Modifying Domains

Procedure

1. Click the System tab.
2. In the left pane, select **Enterprise Directory** .
3. Click the name of a domain in the **Domain** field to display the View Enterprise Directory Domain page for the domain.
   The View Enterprise Directory Domain page displays the domain parameters and the parameters for the Enterprise Directory servers assigned to the domain.
4. Enter the appropriate information and click **Save** to configure the server.

   For more information on the fields, see Enterprise Directory field descriptions on page 163.

5. Click **Reset** to display the settings from the start of this session.
6. Click **Cancel** to exit the page without making any changes.

Modifying LDAP attribute mappings

Before you begin

Follow this procedure only for a combined domain topology. To modify attribute mappings for a split domain topology, see Modifying LDAP attribute mappings for a split domain topology on page 142.

About this task

Avaya one-X® Client Enablement Services reads user and contact information from various enterprise directories, such as Microsoft Active Directory, Microsoft ADAM, IBM Domino, SunOne directory through LDAP.

All enterprise directories do not support the same data schema and allow for customized schemas.

In Client Enablement Services, you can modify the LDAP attribute mapping to establish a relationship matrix between the usages of a field and attribute in the enterprise directory and that of Client Enablement Services.

Client Enablement Services set these attributes for users only when you perform an Enterprise Directory sync.

Procedure

1. Select the **System** tab.
2. In the left pane, select **Enterprise Directory**.
3. On the Enterprise Directory Domains page, click the **Modify LDAP Attribute Mappings** link.
4. On the **Modify LDAP Attribute Mappings** page, select a value from the **LDAP Object Class** drop-down list.

   The value in the **LDAP Object Class** drop-down list field depends on the LDAP you system is integrated with.
5. Select an **Attribute Value** for each corresponding user **Attribute Name**.

   Note:

   - Make sure that the attribute value of **SMGR Login Name** attribute name is same as the login name in System Manager.
   - Do not set the same value for the **E-mail** and **E-mail 2** attribute name. If you select same attribute value for these two fields, the client application

displays an error message when the users logs in to the client application and the server also might stop responding.

6. Click **Save** to modify the mapping to that value.
7. Click **Cancel** to exit the page without making any changes.

Related topics:

Scheduling Enterprise Directory Synchronization on page 130

Modifying the LDAP filter for importing selected users on page 142

Modifying LDAP attribute mappings for a split domain topology

About this task

In a split domain topology, you can only change the service account password.

For more information on split domain topology, see the *Configuring Enterprise Directory for Avaya one-X® Client Enablement Services* section in the *Implementing Avaya one-X® Client Enablement Services* guide.

Procedure

1. Take a back up of the Client Enablement Services database.

   For detailed steps, see Backing up the database on page 240.
2. Stop the Client Enablement Services server.

   For detailed steps, see Stopping Client Enablement Services on page 300.
3. Delete the Client Enablement Services template.
4. Change the passwords in Active Directory.
5. Reinstall the Client Enablement Services template with the new password.

   For detailed steps on installing the template, see the *Installing a solution template* section in the *Implementing Avaya one-X® Client Enablement Services* guide.
6. Restore the database back up.

   For detailed steps, see Restoring the Client Enablement Services database on page 241.

Modifying the LDAP filter for importing selected users

You can import users to Client Enablement Services from the LDAP for user provisioning and enterprise directory contact search. If you import all users from the enterprise directory, the performance of the Client Enablement Services server might be affected. You can filter the users before importing users from the LDAP.

Note:

The LDAP filter support is only available for Microsoft Active Directory and Microsoft ADAM. Do not modify the setting for other LDAP types.

About this task

Using the contact filter, the number of users imported to the database is restricted to the filter you use. Note that the contact filter overrides the LDAP Object Class value administered in the **LDAP Object Class** drop-down list on the Modify LDAP Attribute Mappings page.

Note:

Using an incorrect filter might not yield any results or might make the system unstable. The filter you create must always include the admin users.

Procedure

1. Click the **System** tab.
2. In the left pane, click **Enterprise Directory**.
3. On the Enterprise Directory Domains page, click the **Modify LDAP Filters** link.
4. On the **Enterprise Directory Filters** page, enter the filter in the **Contact Filter** field.

   If you do not enter any value in the **Contact Filter** field, the system applies the default value for the LDAP. The system does not validate the filter expression you enter for correctness.

   - The default filter for Microsoft Active directory is *(objectClass=user)*.
   - The default filter for Microsoft ADAM is *(objectClass=person)*.
5. Click **Save**.
6. Click **Reset**. This restores the settings to the last saved page. If this is a new object, it restores the settings to the default values.

Example

When you use this example filter for Active Directory, Client Enablement Services imports all users whose surname begin with *p*.

(&(objectClass=user)(objectCategory=person)(sn=p))*

Next steps

Perform a full enterprise directory synchronization.

Note:

If you add new users in the LDAP and these users belong to the Client Enablement Services user group but do not satisfy the LDAP filter criteria, the incremental synchronization still imports these users to Client Enablement Services.

Related topics:

Scheduling Enterprise Directory Synchronization on page 130

Modifying LDAP attribute mappings on page 141

License server services

The WebLM server is a Web-based license manager that enables you to track and manage licenses of multiple Avaya software products installed on Avaya one-X® Client Enablement Services from a single location. To track and manage these licenses, WebLM requires a license file of the product that contains product information, such as major release, the licensed features of the product, and the licensed capacities of each feature purchased by the organization.

The system gets into License Error mode when it cannot contact the WebLM server, or there is a problem with the license. In this mode, you can perform any licensed operation, for a grace period of 30 days.

After the grace period of 30 days in the License Error mode is over, the system enters the License Restricted mode. If the License has not been renewed or the error has not been fixed, you cannot do the following functions in the License Restricted mode:

- You cannot provision new users from the administration application.
- If you disable an existing user, you cannot enable the user again till the License is in Normal mode.
- Users cannot log in the client application.

  The client application displays an error message `Please confirm your login information and try again`.

  You can verify the actual reason from the trace.log file that mentions `License grace period is over, please contact administrator`.

You can use either the WebLM of a remote System Manager WebLM or the System Platform WebLM for licensing. Use the local WebLM server only when the System Manager WebLM is not available.

- If you have selected the System Platform WebLM during installation, use the port 8443.
- If you have selected the System Manager WebLM during installation, use the port 52233.

When you provision a user, one the system consumes one license. When you unprovision or delete a user, the system releases the user license.

Related topics:

Configuring the license server on page 145
License server field descriptions on page 167

Configuring the license server

Procedure

1. Click the **System** tab.
2. In the left pane, select **License Server**.
3. On the License Server Configuration page, enter the appropriate information and click **Save** to configure the server.

   For more information on the fields, see License server field descriptions on page 167.
4. Click **Reset** to display the settings from the start of this session.

Related topics:

License server services on page 144
License server field descriptions on page 167

SIP Local

To build a link between Communication Manager and Avaya one-X® Client Enablement Services, we need a system to act as a Local SIP and a system to act as a Remote SIP. In this link, Client Enablement Services is the Local SIP system and Communication Manager is the Remote SIP system.

To establish a secure connection between Client Enablement Services and Communication Manager through Session Manager, configure the **Port** to 5061 and select the **Secure Port** check box.

Related topics:

Telephony servers and Auxiliary servers on page 41
Configuring the SIP local server on page 146

Configuring the SIP local server

Procedure

1. Select the **System** tab.
2. From the left pane, select **SIP Local**.
3. Enter the appropriate information and click **Save** to configure the SIP Local server.

   For more information on fields, see SIP Local field descriptions on page 179.
4. Click **Reset** to restore the settings to the last saved page.

Mobile applications

You must administer mobile releases on Avaya one-X® Client Enablement Services for Avaya one-X® Mobile users. You can download the mobile binaries package from the Avaya support site and then upload them through the Client Enablement Services server to the mobile software download site. This configures the Client Enablement Services system with the characteristics of mobile releases and allows you to control release availability to the user. Users can download software updates and upgrades for their mobiles from a mobile software download site which provides mobile client releases to the end users.

Note:

For IPhone also, you need to upload a package to the mobile software download site. This package does not contain binaries. It contains information on supported mobile releases. Users can download the binary for IPhone from App Store.

Following are the high-level steps you should follow:

1. Configure the mobile application URL and port.
2. Upload the mobile application package to mobile software download site.
3. Configure the mobile application details.

When you upload a new release or make active a previous version of a mobile application in the administration application, a system generated message, SMS and e-mail, is sent to the user. They receive two messages, one containing the mobile software download site URL and another containing the Handset server IP and port. The mobile software download URL provides the user access to the mobile software download site where the mobile releases are available for download. Users need the Handset server IP and port to log in to the Handset server.

Note:

You should configure the Handset server in the Client Enablement Services administration application before configuring mobile applications. The IP address and Port of the Handset server is required for sending the SMS about the application server URL to the user.

You can also decide to make the software updates mandatory for the users. They get a reminder for N days after which the software update is mandatory. The notifications can be controlled by the System profile and Group profiles by enabling or disabling the software update notifications property.

Related topics:

Configuring the mobile application URL on page 147
Uploading mobile applications on page 148
Configuring mobile application details on page 148

Configuring the mobile application URL

About this task

The Handset server acts as an interface between the mobile application and the Avaya one-X® Client Enablement Services server. The mobile application connects over SSL to the Handset server, and then the Handset server connects to the Client Enablement Services server for all kind of requests such as login, searching history, downloading voice mails, making callback calls, and enterprise directory search.

Procedure

1. Click the **System** tab.
2. In the left pane, select **Mobile Applications**.
3. On the Mobile Applications page, enter the **Url** and **Port** details.
4. Click **Save** to save the changes.
5. Click **Reset** to restore the settings to the last saved page.

Uploading mobile applications

Before you begin

You must configure the mobile application URL and Port details before uploading a mobile application.

About this task

You can upload one or more mobile application for a manufacturer and model, but only one mobile application can be active at a time. If you have to upload a new release for the same manufacturer and model and make it active, you must first make the active mobile application inactive from the administration application.

Procedure

1. Download the mobile application package zip file, which contains the mobile binary and the properties file, from the Avaya support site.
2. Copy the zip file in the `/opt/avaya/1xp/mobileapps` directory on the Client Enablement Services server.
3. In the Client Enablement Services administration application, click the **System** tab.
4. In the left pane, select **Mobile Applications**.
5. On the Mobile Applications page, enter the mobile application file name, which is the name of the zip file, in the **Mobile application filename** field.
6. Click **Upload mobile applications**.

   The mobile application is uploaded to the mobile software download site from where the user can download them. The Mobile Applications page displays the details of the mobile application you uploaded such as manufacturer, model, release status, and version.

   You must set the **Release Status** of an upload mobile application to **Active**. After you do this, users can view the mobile application on the mobile software download site.

Configuring mobile application details

Before you begin

You must upload the mobile application package to the mobile software download site. Only, then you can configure the mobile application details.

About this task

The Mobile application binaries are uploaded as a ZIP file. The Zip file contains mobile application binaries and their characteristics (properties). When you upload a mobile application binary, the details of the mobile application appear in the Mobile Applications page on the mobile software download site.

Procedure

1. Click the **System** tab.
2. In the left pane, select **Mobile Applications**.
3. On the Mobile Applications page, click the link in the **Version** column to display the Mobile Application Configuration page for a mobile application.
4. On the Mobile Application Configuration page, enter the appropriate information.

   For more information on the fields, see Mobile application field descriptions on page 180.
5. Click **Save** to save the changes.
6. Click **Reset** to restore the settings to the last saved page.
7. Click **Cancel** to exit the page without making any changes.
8. Click **Delete** to delete the mobile application.

SMS domains

SMS domains is the list of SMS domain providers. The SMS domains are used to build the SMS addresses of users. This address is stored in the user configuration and used to send SMS messages to the user.

The list of SMS domain in the administration application is the default list. You should add a new SMS domain when the default list does not contain the SMS provider.

Related topics:

Adding SMS domains on page 150
Modifying SMS domains on page 150

Adding SMS domains

Procedure

1. Click the **System** tab.
2. In the left pane, select **SMS Domains**.
3. On the SMS Domains page, click **Add new SMS domain**.
4. On the Add SMS Domain Configuration page, enter the appropriate information.

   For more information on the fields, see SMS domains field descriptions on page 181.
5. Click **Ok** to add the SMS domain.
6. Click **Reset** to restore the page settings.
7. Click **Cancel** to exit the page without saving the changes.

Modifying SMS domains

Procedure

1. Select the **System** tab.
2. From the left pane, select **SMS Domains**.
3. On the SMS Domains page, click the link in the **SMS Domain** column to modify the SMS domain for a carrier.
4. On the SMS Domain Configuration page, enter the appropriate information.

   For more information on the fields, see SMS domains field descriptions on page 181.
5. Click **Save** to save the changes made to the SMS domain.
6. Click **Reset** to restore the page settings.
7. Click **Delete** to delete the SMS domain.

Notification

Notification service sends notifications using the SMTP protocol as a mail to the client users. You can set up an SMTP connection over transport layer security (TLS) using an SSL certificate. Obtain a certificate from the SMTP server using a tool such as openssl, and upload the certificate to the Avaya one-X® Client Enablement Services server while configuring the notification server. Notifications are in a queue when the notification service tries to establish a connection with the SMTP server. If the notification is not sent within the maximum connect period duration, the message delivery fails. The SMS e-mail address is a facility provided by mobile service providers to send SMS notifications.

The system can send notifications to a user only when the following settings are configured in the administration application:

- The **SMS notification** field in the **Voice Messaging** resource assigned to the user is set to **all** or **priority**.
- The **Mobile Number** and the **Mobile SMS Address** fields are defined for a user in the **Mobile Telephony** resource assigned to the user.

If the **SMS notification** field is set to **all** or **priority**, the system notifies the user of a new voice message. The notification message body includes the name of the caller and the duration of message. The system also notifies users about software download information when there is a mobile client software update.

Related topics:

System profile and Group profile field descriptions on page 92
Assigning a Mobile Telephony resource to a user on page 113
Assigning a Voice Messaging resource to a user on page 115
Modifying the notification service on page 151
Installing the certificate for TLS connection to the Notification server on page 152

Modifying the notification service

Procedure

1. Select the **System** tab.
2. From the left pane, select **Notification**.
3. On the Modify Notification Service page, enter the appropriate information and click **Save** to save the changes made to the notification service.

   For more information on fields, see Notification service field descriptions on page 182.

4. Click **Browse** and select the certificate you obtained from the SMTP Server.

   You must copy the .crt SSL certificate file from the SMTP server to your system.
5. Click **Upload**.
   The system uploads the .crt SSL certificate file to the WebSphere Trust Store.
6. Click **Save** to save the changes.
7. Click **Reset** to display the settings from the start of this session.

Related topics:

Installing the certificate for TLS connection to the Notification server on page 152

Installing the certificate for TLS connection to the Notification server

To establish a TLS connection to the Notification server, you must extract the certificate from the SMTP server, and install the certificate on the Client Enablement Services server.

About this task

You must first create a script to retrieve the certificate from the SMTP server, run the script, and then install the certificate on the Client Enablement Services server.

You can use OpenSSL to retrieve the certificate from the SMTP server.

Procedure

1. Create a script file to retrieve the certificate from the SMTP server. For example, *retrieve-cert.sh*.

   Content of the *retrieve-cert.sh* script file:

```
 #!/bin/sh
 #
 # usage: retrieve-cert.sh remote.host.name [port]
 #
 REMHOST=$1
 REMPORT=$2

  echo |\
  openssl s_client -starttls smtp -crlf -connect ${REMHOST}:${REMPORT}
2>&1 | sed -ne '/BEGIN CERTIFICATE/,/END CERTIFICATE/p' > smtpCert.pem
```

2. On the Client Enablement Services server, run the *retrieve-cert.sh* script using the command: **`# ./retrieve-cert.sh <IP_Address_of_SMTP_Server> <smtp_port>`**

   Note:

   SMTP port value must always be 25.
3. Log in to the Client Enablement Services administration application.

4. In the left pane, select **Notification**.
5. On the Modify Notification Service page, click **Browse** and select the certificate you obtained from the SMTP Server.
6. Click **Upload**.
   The system uploads the .crt SSL certificate file to the WebSphere trust store.
7. Click **Save** to save the changes.

Related topics:
Modifying the notification service on page 151

SNMP Traps

Avaya one-X® Client Enablement Services can notify Network Management Stations (NMS) about alarm events by sending SNMP Traps.

Use the SNMP Traps option to define:

- alarm events for which you want to send SNMP traps
- destinations where you want to send the SNMP traps

Related topics:
Configuring SNMP traps on page 153
SNMP Traps field descriptions on page 168

Configuring SNMP traps

Procedure

1. Select the **System** tab.
2. From the left pane, select **SNMP Traps**.
3. On the SNMP Traps page, enable or disable the SNMP Traps as desired.
   - Select the check box for each SNMP Trap you want to enable.
   - Click **Check All** to enable all the SNMP Traps on the list.
   - Click **Uncheck All** to disable all the SNMP Traps on the list.
4. Click **Save** to save your changes.

5. Click **Refresh** to display the settings from the start of this session.

Related topics:

SNMP Traps on page 153
SNMP Traps field descriptions on page 168

SNMP Destinations

SNMP Destinations are devices to which you can send specified traps, also called event notifications. On Avaya one-X® Client Enablement Services, these devices can either be the Avaya Services Security Gateway (SSG) or industry standard Network Monitoring Software (NMS) such as HP Openview or IBM Tivoli. Use this option to define specified destinations when certain events take place on Client Enablement Services.

Related topics:

Listing SNMP destinations on page 154
Adding SNMP destinations on page 155
Adding an SNMP destination for SAL gateway on page 155
Modifying SNMP destinations on page 156
SNMP destinations field descriptions on page 168

Listing SNMP destinations

Procedure

1. Click the **System** tab.
2. In the left pane, select **SNMP Destinations**.
3. On the SNMP Destinations page, click the name of an SNMP destination in the **Handle** field to display the Modify SNMP Destination Configuration page for the destination.

Related topics:

SNMP Destinations on page 154
SNMP destinations field descriptions on page 168

Adding SNMP destinations

Procedure

1. Select the System tab.
2. From the left pane, select **SNMP Destinations**.
3. On the SNMP Destinations page, click **Add New SNMP Trap Destination** to display the Add SNMP Destination Configuration page.
4. Enter the appropriate information and click **OK** to add the server.

   For more information on the fields, see SNMP destinations field descriptions on page 168.
5. Click **Reset** to display the settings from the start of this session.
6. Click **Cancel** to exit the page without making any changes.

Related topics:

SNMP Destinations on page 154

SNMP destinations field descriptions on page 168

Adding an SNMP destination for SAL gateway

About this task

You need to configure traps to be sent to SAL, if Avaya provides maintenance coverage for the system and alarm notification to Avaya is required. The SAL gateway acts like an NMS. It captures the traps and sends them to Avaya Services. The only difference is that SAL gateway uses INADs traps. This is done by setting the **Device** to **SSG**.

Procedure

1. Select the **System** tab.
2. From the left pane, select **SNMP Destinations**.
3. On the SNMP Destination page, click **Add New SNMP Trap Destination**.
4. On the Add New SNMP Destination Configuration page, enter following details in the fields.
   - **Handle**: cdomSALGW
   - **Enable**: selected
   - **Device**: SSG because the traps are sent in INADS format

- **Host**: IP address of the SAL Gateway on System Platform
- **Port**: 162 (default)
- **Notification Type**: Trap
- **SNMP version**: 2c

Note:

Leave all other fields blank or set defaults to **None**.

5. Click **OK** to save your changes.

   The system displays a new SAL Gateway SNMP trap destination in the list of SNMP Trap destinations.

Next steps

You should generate a test trap after specifying the SNMP Trap destination to test that the SAL gateway and Avaya one-X® Client Enablement Services are configured properly. When you clean up the performance statistics, Client Enablement Services generates an SNMP trap. To do this, perform the following:

1. Select the **Scheduler** tab.
2. From the left pane, select **Statistics Cleanup**.
3. Click **Run Now** in the **Performance Statistics Cleanup Settings**.

   The system displays the task status.

Related topics:

Scheduling Statistics Cleanup on page 133

Modifying SNMP destinations

Procedure

1. Click the System tab.
2. In the left pane, select **SNMP Destinations**.
3. On the SNMP Destinations page, click the name of an SNMP Destination in the **Handle** field.

   The system displays the Modify SNMP Destination Configuration page for the destination.
4. Enter the appropriate information and click **Save** to update the destination.

   For more information on the fields, see SNMP destinations field descriptions on page 168.
5. Click **Reset** to display the settings from the start of this session.

6. Click **Cancel** to exit the page without making any changes.
7. Click **Delete** to delete the destination from Avaya one-X® Client Enablement Services.

Related topics:

SNMP Destinations on page 154

SNMP destinations field descriptions on page 168

Statistics configuration

Use the Statistics Configuration option to configure the collection of Performance Statistics (system level and user level) and Usage Statistics (user level) on Avaya one-X® Client Enablement Services. You can define how often to collect these statistics and how long to keep them.

Performance statistics captures the details of performance of the system and stores the data in the performanceStatistic table in the Client Enablement Services database. The Statistics information is sent to logs if **Aspect Logging** for **Statistics** is enabled in the **System** > **Logging** page. Use the **Scheduler** > **Statistics cleanup** settings to specify the cleanup settings for performance statistics.

Feature Usage statistics captures the details of usage of each feature by the users and stores the data in the featureStatistic table. You can send the Feature Usage statistics information to logs and specify the cleanup setting in similar way as Performance statistics.

Related topics:

Sample logs for statistics on page 157

Configuring statistics on page 159

Statistics field descriptions on page 170

Sample logs for statistics

Log information for Performance Statistics

Performance Statistics are gathered for client side operations as well as for system services. All time intervals in the sample are shown in milliseconds. The average number is computed as per the collection interval configured for Performance Statistics.

A client side operation log for statistics contains the Client SDK context description. The Operation description contains information for the type of service invoked or operation executed on behalf of the user.

Performance Statistics log snippet for a client side operation:

```
[9/3/10 8:23:18:146 PDT] 00000023 statistics 1
Operation(ClientSDK,smoke1.1,adapter.type=MM,adapter.version=1.1,service.t
ype=voicemessaging,service.type.version=1.1,provider.name=MM,provider.vers
ion=1.1) Statistics(min=156 max=156 average=156 collectionTime=9/3/10 8:23
AM)|Thread=WorkManager.StatisticsServiceRequestWorkManager : 0
```

Performance Statistics log snippet for a service operation:

```
[9/3/10 9:08:36:556 PDT] 00000a1b statistics 2 Update stats cache:
TimedOperation(Telephony
Service,CM-34.33,perf.operation.tel.extcontrol,getSmsDoaminsByCountry)
Current Stats(RunningTime[40], #TimesRan[1]) Cumulative
Stats(Min[40],Max[40],Total[40],Count[1])|Thread=Thread-132
```

```
[9/3/10 9:08:36:621 PDT] 00000a27 statistics 2 Update stats cache:
TimedOperation(Telephony
Service,CM-34.33,perf.operation.tel.extcontrol,getMobileAppsByLanguage)
Current Stats(RunningTime[16], #TimesRan[1]) Cumulative
Stats(Min[16],Max[40],Total[56],Count[2])|Thread=Thread-142
```

```
[9/3/10 9:09:19:051 PDT] 00000023 statistics 1 Operation(Telephony
Service,CM-34.33,perf.operation.tel.extcontrol) Statistics(min=16 max=40
average=28 collectionTime=9/3/10 9:09 AM)|
Thread=WorkManager.StatisticsServiceRequestWorkManager : 0
```

Note:

The `Update stats cache` log entries show individually timed operations inside a collection interval.

Log information for Feature Statistics

Feature Usage statistics captures the details of usage of each feature by the users. The usage count is the number of times the feature is used in the collection interval configured for Feature Statistics.

Feature Statistics log snippet for user *smoke1.1*:

```
[9/3/10 8:22:16:342 PDT] 00000023 statistics 1 user=smoke1.1
feature=feature.telephony.stationcontrol,StationControl usage-count=1
collectionTime=9/3/10 8:22 AM|
Thread=WorkManager.StatisticsServiceRequestWorkManager : 0
```

```
[9/3/10 9:07:17:074 PDT] 00000023 statistics 1 user=smoke1.1
feature=feature.contactsearch,getChunkedMatchingContactsByName usage-
count=2 collectionTime=9/3/10 9:07 AM|
Thread=WorkManager.StatisticsServiceRequestWorkManager : 0
```

Configuring statistics

Procedure

1. Select the System tab.
2. From the left pane, select **Statistics**.
3. On the Statistics Configuration page, enter the appropriate information and click **Save** to configure the server.

   For more information on the fields, see Statistics field descriptions on page 170.
4. Click **Reset** to display the settings from the start of this session.

Related topics:

Statistics configuration on page 157

Statistics field descriptions on page 170

Logging

Avaya one-X® Client Enablement Services provides the following types of Logging for system analysis and debugging purposes.

- General high-level system logging
- Protocol-level logging
- Aspect-level, also called component-level, logging by user
- Non-Avaya or Internal logging

Logging provides the following types of log files:

- `trace.log`. Contains General, Protocol, and Aspect level logging.
- `systemOut.log`. Contains General level logging.
- `stopServer.log`. Contains Service Stop logs.
- `startServer.log`. Contains Service Start logs.
- `systemErr.log`. Contains Error logs.

All the log files are generated at the location: `/opt/IBM/WebSphere/AppServer70/profiles/default/logs/server1/`

Note:

If you are an auditor, you do not have access to the Logging page. The system displays a WebSphere administration rights message. Click the back icon on the browser to return to the previous page.

Related topics:

Downloading log files on page 160
Configuring logging on page 160
Logging field descriptions on page 171
Managing disk space on the Avaya one-X Client Enablement Services template on page 243

Downloading log files

Procedure

1. Click the **System** tab.
2. In the left pane, select **Logging**.
3. On the Logging Configuration page, in the **Download Log Files** field, click **All Log Files**.
   The system opens the **File Download** dialog box. This dialog box displays the following:
   - A message: **Do you want to open or save this file?**
   - Name: *log file name*
   - Type: *WinZip File*
   - From: *IP address of the Administration application*
4. Click **Open** to open the log files on your computer.
5. Click **Save** to save the log files to your computer.
6. Click **Cancel** to close the dialog box.

Configuring logging

Procedure

1. Click the System tab.

2. In the left pane, select **Logging**.
3. On the Logging Configuration page, enter the appropriate information and click **Save** to configure the server.

   For more information on the fields, see Logging field descriptions on page 171.
4. Click **Reset** to display the settings from the start of this session.

Related topics:

Logging on page 159

Logging field descriptions on page 171

JDBC connector

Avaya one-X® Client Enablement Services uses Java Database Connectivity (JDBC), the SQL database interface, to gain access to the Client Enablement Services DB2 database. JDBC is the industry standard for database independent connectivity between the Java programming language and a wide range of databases. In Client Enablement Services, the JDBC option administers connections to the Client Enablement Services database.

Related topics:

Configuring JDBC on page 161

JDBC field descriptions on page 178

Configuring JDBC

About this task

To configure JDBC connections to the Avaya one-X® Client Enablement Services database, you must be logged in to the WebSphere administration page.

Procedure

1. Click the System tab.
2. From the left navigation pane, select **JDBC**.
3. On the JDBC Configuration page, enter the appropriate information and click **Save** to configure the server.

   For more information on the fields, see JDBC field descriptions on page 178.
4. Click **Reset** to display the settings from the start of this session.

Related topics:

JDBC connector on page 161
JDBC field descriptions on page 178

System field descriptions

Related topics:

General Settings field descriptions on page 162
Enterprise Directory field descriptions on page 163
License server field descriptions on page 167
SNMP Traps field descriptions on page 168
SNMP destinations field descriptions on page 168
Statistics field descriptions on page 170
Logging field descriptions on page 171
JDBC field descriptions on page 178
SIP Local field descriptions on page 179
Mobile application field descriptions on page 180
SMS domains field descriptions on page 181
Notification service field descriptions on page 182

General Settings field descriptions

The General Settings page displays the following fields:

Name	Description
Administrator Contact URL	The Web address or the e-mail address used to contact the system administrator or technical support in the event of an issue with Avaya one-X® Client Enablement Services.
Product ID (10 digits)	The product ID code that is used for alarming and identifying which unique product is generating the alarm. This number is issued when Client Enablement Services is registered for technical support.
Presence domain Rule From	Domain of the Client Enablement Services system.
Presence Domain Rule To	Domain of the Presence Services system.

Name	Description
Application Server Version	Version of the Client Enablement Services system.
Database Server Version	Version of the database.
Save	Exits the page with the current settings saved.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.

Related topics:

General settings on page 137
Configuring general settings on page 137
Enterprise Directory field descriptions on page 163

Enterprise Directory field descriptions

The Enterprise Directory Domains page displays the following fields:

Name	Description
Domain	Fully qualified domain name configured on the enterprise directory server. For example, enter the **User** domain as `<`*NNNNN*`>.xyz-corp.com`, and the **Resource** domain as `<`*nnnn*`>pptdomain.xyz-corp.com`. The **Contact** domain is the same as the **User** domain. You can add the Contact domain with another name. However, you cannot add a User or Resource domain.
Type	Indicates how the domain is used. The same domain can be used in more than one way. • **User**. Indicates the domain contains the Avaya one-X® Client Enablement Services users. There is only one user domain. You cannot change this domain. • **Resource**. Indicates the domain contains the Client Enablement Services security groups. There is only one resource domain. You cannot change this domain. • **Contact**. Indicates the domain contains enterprise address book information. The

Name	Description
	user domain is always the first contact domain. You can add up to four more contact domains.
Server	The IP address of the enterprise directory server for the domain.

The Add Enterprise Contact Domains page displays the following fields:

Name	Description
Host	IP address of the computer that hosts the enterprise directory server. The host value can also be the FQDN.
Port	Port that the Client Enablement Services server uses to communicate with the enterprise directory server
Login ID	The log-in ID used by the enterprise directory server.
Password	The password associated with the Login ID used by the enterprise directory server.
Confirm	Re enter the password associated with the Login ID used by this server.
Base DN	The Distinguished Name (DN) of a node in the domain that identifies which part of the domain is used. If blank, the entire domain is used. You can change this value to improve search performance. However, changes may exclude information from other parts of the domain.
Page Size	The number of names returned by the enterprise directory server per query.
Range Size	The number of values for an attribute that are returned by the enterprise directory server per query. The attributes include names and phone numbers. For example, if a security group contains 1,000 members and if you enter 200 in the **Range Size** field, you can retrieve the details of 200 members at a time.
OK	Exits the page with the current settings saved.

Name	Description
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.

The View Enterprise Directory Domain page displays the following fields:

Name	Description
Domain	Fully qualified domain name configured on the enterprise directory server. For example, *users.domain.xyz corp.com*.
Type	Indicates how the domain is used. The same domain can be used in more than one way. • **User** domains are fixed. There can only be one domain, and the domain attributes, such as name and type, cannot be changed. **User** domains can contain user records, security group information, and contact information. • **Resource** domains are fixed as well and they contain security group information. • **Contact** domains can be added and modified. They contain the contact information used by users.
Description	Description to identify the enterprise directory server.
Enable	If selected, enables the Enterprise Directory domain.
Base DN	The Distinguished Name (DN) used by the LDAP server. For example, for ADAM *DC=sysucd,DC=Avaya,DC=com*; and for SunOne *DC=Avaya,DC=com*. **Note:** If the LDAP type is IBM Domino Server or Novell eDirectory, do not enter any value in the **Base DN** field.
Login ID	The log-in ID used by the enterprise directory server.
Password	The password associated with the Login ID used by the enterprise directory server.

Name	Description
Confirm	Re enter the password associated with the Login ID used by this server.
Server	The number assigned to the enterprise directory server connected to the domain to determine the failover order. In this release, you can add only one enterprise directory server.
Host	IP address of the computer that hosts the enterprise directory server. The host value can also be the FQDN.
Port	Port that the Client Enablement Services server uses to communicate with the enterprise directory server
Secure Port	If selected, the port number used by the Client Enablement Services server is secure.
Page Size	The number of names returned by the enterprise directory server per query.
Range Size	The number of values for an attribute that are returned by the enterprise directory server per query. The attributes include names and phone numbers. For example, if a security group contains 1,000 members and if you enter 200 in the **Range Size** field, you can retrieve the details of 200 members at a time.
Save	Exits the page with the current settings saved.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.

Related topics:

Enterprise Directory domains on page 138

General Settings field descriptions on page 162

License server field descriptions

Name	Description
Host	IP address of the computer that hosts the enterprise directory server. The host value can also be the FQDN.
Port	Port that the Client Enablement Services server uses to communicate with the enterprise directory server
Secure Port	If selected, indicates the system is configured to use a secure connection for the License server.
URL	The Web address where the WebLM server is installed. • If you are using the System Manager WebLM, enter `https://<SMGR_IP_OR_FQDN>:52233/WebLM/LicenseServer` • If you are using the System Platform WebLM, enter `https://<IP_OR_FQDN of the CDOM>:8443/WebLM/LicenseServer`
Mode	The status of the current mode of the WebLM server as **Error**, **Restricted**, or **Normal**.
Mode Last Changed	The date and time that the license mode of the WebLM server last changed.
Server Up	The running status of the WebLM server as **Yes** or **No**. If the status is set to **No**, the WebLM server is unreachable.
Server Last Changed	The date and time that the running status of the WebLM server changed.
Product Name	The name of the product, Client Enablement Services.
Feature Name	The name of the feature which provides the number of licensed users.
Desired Units	The requested number of license units.
Acquired Units	The acquired number of license units. Used to determine if the number of licenses were over provisioned.

Name	Description
Save	Saves the current settings on the page.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.

Related topics:

License server services on page 144
Configuring the license server on page 145

SNMP Traps field descriptions

Name	Description
Trap Name	The unique name assigned to the SNMP Trap (event notification).
Description	Brief description of the SNMP Trap.
Check All	Selects all SNMP Traps and enables them. Select the check box next to the SNMP Trap to enable that trap only.
Uncheck All	Selects all SNMP Traps and disables them. Select the check box next to the SNMP Trap to disable that trap only.

Related topics:

SNMP Traps on page 153
Configuring SNMP traps on page 153

SNMP destinations field descriptions

Name	Description
Handle	The unique name assigned to the server by the administrator.
Enable	Enables the configuration of the SNMP trap.
Device	The device to which traps are generated.

Name	Description
	The selections are: • **SSG**. The Avaya Services Security Gateway (SSG). Only INADS traps are sent here. • **NMS**. Industry standard Network Monitoring Software (NMS), such as HP Openview or IBM Tivoli. INADS traps are not sent here.
Host	The IP Address of the device that receives the traps.
Port	The TCP or UDP port number used when sending the traps.
Notification Type	Indicates the method of notification for this destination. The selections are: • **Trap**. Notification is sent using the SNMP Trap command. There is no handshake with the receiver of the trap to verify it was received. Trap can be used with all versions of SNMP. • **Inform**. Notification is sent using the SNMP Inform command. The receiver sends a response packet to indicate the notification was received. Inform can only be used with SNMP versions 2c and 3.
SNMP Version	Indicates the version of SNMP to be used for this destination. You can select from: 1, 2c, and 3.
User Name	Indicates the user name associated with this destination. For security reasons, you must not use the words "public" or "private" in this field.
Security Level	Indicates the security level assigned to this destination. The selections are: • **None**. Do not use the authentication and privacy fields. • **Authentication**. Use the authentication fields only.

Name	Description
	• **Privacy**. Use the privacy fields only. • **Authentication and Privacy**. Use both the authentication and privacy fields.
Authentication Protocol	Indicates the Authentication protocol to use to authenticate SNMP version 3 messages. The selections are **None**, **MD5**, or **SHA**.
Authentication Password	Indicates the Authentication password for authenticated SNMP version 3 messages.
Confirm	Re enter the Authentication password for verification.
Privacy Protocol	Indicates the Privacy Protocol used to encrypt SNMP version 3 messages. Select from **DES**, **AES128**, **AES198**, or **AES256**.
Privacy Password	Indicates the Privacy password for encrypted SNMP version 3 messages.
Confirm	Re enter the Privacy password for verification.
OK	Saves the current settings on the page.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Deletes the SNMP destination.

Related topics:

SNMP Destinations on page 154
Listing SNMP destinations on page 154
Adding SNMP destinations on page 155
Modifying SNMP destinations on page 156

Statistics field descriptions

The Statistics configuration page displays the following fields for Performance statistics and Feature Usage statistics:

Name	Description
Enable Collection	Indicates that the system collects the specified statistics, Performance or Feature Usage or both.
Collection Interval	The duration in which the system collects the specified statistics. Select from 1 to 240 minutes.
Retention Period	The number of days that the system keeps the collected statistics. Select from 1 to 90 days.
Save	Saves the current settings on the page.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.

Related topics:

Scheduling Statistics Cleanup on page 133
Statistics configuration on page 157
Configuring statistics on page 159

Logging field descriptions

Name	Description
General Logging	Client Enablement Services logging provides high-level system information. Generally, the system writes the logs to `SystemOut.log` and also to `trace.log` log files if you activate the either Protocol, Aspect, or Other Logging.
Level	The level of **General Logging**. You can select the level from the following options: **All**, **Fatal**, **Error**, **Info**, **Off**, or **Warning**.
Protocol Logging	Low-level logging that debugs issues with the protocols used by Client Enablement Services. The system generates messages for debugging protocol exchanges. For example, SMTP or SIP. The system writes the logs only to `trace.log`.

Name	Description
Protocol	The protocol for which you want to run logging. Select a protocol from the drop-down list.
Level	The level of logging to run for protocol logging levels. You can select the level from the following options: **Summary**, **Traffic**, or **Off**.
List of Current Protocol Loggers	The Protocol Level logger. • **api**. Debugs general client issues. The client API uses this protocol in Client Enablement Services. • **bcapi**. Debugs conferencing issues. Conferencing services use this protocol to connect to Conferencing. • **cmapi**. Debugs Telephony issues. For example, Other Phone log in problems and Extension to cellular issues. • **cmcontact**. Reports the communication between the Telephony Adapter and the Contact Services. • **cmstore**. Reports database information. Telephony services use this protocol to report information that is stored in the database. • **contlogtrim**. Used by the service that trims Contact Logs. • **crypt**. Used by Encryption or Decryption methods. • **fwclient**. Used to view traffic between client and service layers. The protocol used by framework client. • **fwintercept**. Used by Service Framework during method intercept. • **fwservice**. Used by Service Framework. • **imap**. Used to connect to Modular Messaging. Use this protocol to debug messaging problems. • **jtapi**. Used to connect to Communication Manager. Telephony services use this as one of the protocols to connect to Communication Manager. Use this to resolve Telephony issues.

Name	Description
	• **lps**. Debugs Presence issues. Presence service uses this protocol to connect to the Avaya Aura®Presence Services. • **snmp**. Used by Alarm service to issue SNMP notifications. • **spectel**. Debugs Conferencing issues. Conferencing services use this as one of the protocols to connect to Conferencing. • **weblm**. Debugs licensing issues. The Client Enablement Services uses this protocol to connect to the licensing services. • **audiotrns**. Captures the protocol messages between audio transcoding service and the transcoding server. • **smtp**. Captures SMTP messages for notification service. • **onexsip**. Captures all SIP messages sent across SIP-CM adapter service and Session Manager/ direct CM SIP.
Aspect Logging	Low-level logging used to debug issues with the Client Enablement Services components. The system generates messages for debugging subsystem activity. For example, Telephony or Conferencing. This can be enabled for specific Users in the system. The system writes the logs only to `trace.log`.
Aspect	The Aspect for which you want to run logging. Select a protocol from the drop-down list.
Level	The level of logging to run for aspect logging levels. You can select the level from the following options: **Summary**, **Detail**, **Off**.
User ID	The identifier of the user for whom you want to debug a component issue. For example, you can debug a Telephony issue for a selected user. To turn logging on, the user must be specified.

Name	Description
List of Current Aspect Loggers	The available aspect loggers that help you to debug issues with protocols. • **admincli**. Logs the admin CLI client activities. By default, the command line client saves the logs in the `acp_admin_cli.log` file in the logs directory of the WebSphere profile. • **api**. Logs all the activity in the layer of code that the clients interact with. This is the Client API aspect that can be used to debug client issues. • **bulk**. Logs bulk operations information such as bulk import or export of users. • **client**. Supports all clients integrated with Client Enablement Services. It is an end-client aspect that can be used to debug client issues. • **cmtelephony**. Logs Communication Manager telephony activity for a specified user. If you do not specify a user, this logs information about the service. If you specify a user, this logs information about the user interaction with the telephony adapter. • **contactlog**. Used by the Service that writes Contact Logs. • **dirstores**. Logs the Directory Service activities. It reports information about the interactions with the LDAP providers, such as Directory Synchronization tasks and user group membership lookup. • **framework**. Logs Service Framework activities around ServiceBean and ServiceRegistry. • **fwadmin**. Logs Service Framework application for Server Management Operations (administration). • **fwasync**. Logs Service Framework asynchronous method invocation. • **fwproxy**. Logs Service Framework proxy interface operations. • **ldapclient**. Specific for the LDAP client used to connect to the LDAP server. It logs

Name	Description
	low-level LDAP information, such as queries to LDAP server and responses. • **licensing**. Logs License Server activity. • **mmclient**. Logs activities, such as request and response, to and from Modular Messaging (voice messaging) service over client channel. • **mmldap**. Logs activities related to Modular Messaging directory synchronization. • **mmservice**. Logs activities on Modular Messaging (voice messaging) service. • **mmsystem**. Logs activities, such as request and response, to and from Modular Messaging (voice messaging) service over system channel. • **mxclient**. Logs activities, such as request and response, to and from Conferencing (bridge conferencing) service over client channel. • **mxservice**. Logs activities on Conferencing Exchange (bridge conferencing) service. • **mxsystem**. Logs activities, such as request and response, to and from Conferencing (bridge conferencing) service over system channel. • **prsncclient**. Logs activities, such as request and response, to and from Presence service over client channel. • **prsncservice**. Logs activities related to Presence service. • **prsncsystem**. Logs activities, such as request and response, to and from Presence service over system channel. • **statistics**. Logs runtime statistics collected by statistics service. At summary level, logs statistics at every collection interval. By default, this interval is 15 minutes. At detail level, logs statistics as they are collected. • **user**. Logs User Service activities. • **userassistant**. Captures user assistant logs for all activities such as marking non-

Name	Description
	VIP call blocking, publishing presence on mode changes and so on. • **audiotransclient**. Captures audio transcoding service client channel operations such as request for transcoding and so on. • **audiotransservice**. Captures audio transcoding service for server connectivity with transcoding server and overall service functionality. • **audiotranssystem**. Captures audio transcoding service for system channel functionality. • **notificationClient**. Captures notification service client channel functionality primarily for checking send notification operation. • **notifictationSystem**. Captures notification service system channel functionality. • **notificationAdmin**. Captures notification service admin channel functionality. This involves capturing requests for service configuration changes. • **notificationSMTPProvider**. Captures logs for SMTP server connectivity and overall send notification operation.
Other Loggers	Low-level logging used to debug issues with non-Avaya and internal components. The system internal log messages that may be useful during development. The logs are written only to `trace.log`. This information is provided by the Services that support the product. **Note:** Do not set the level of ***** logger to **All**. This results in CPU usage spike. Set the level to either **Off** or **Info**.
Logger	The name or identifier of the logger for which to run logging. For example, org.springframework.

Name	Description
Level	The level of logging to run for non-Avaya or internal loggers. You can select the level from the following options: **Fatal**, **Severe**, **Warning**, **Audit**, **Info**, **Config**, **Detail**, **Fine**, **Finer**, **Finest**, **All**, or **Off**.
List of Current Other Loggers	The other loggers, non-Avaya or internal, that are available for use to debug issues with components such as WebSphere or the Spring framework.
Trace Log File Settings	Trace-level logging.
File Name	The name of the trace log file. For example, ${SERVER_LOG_ROOT}/trace.log.
Maximum number of historical files	The maximum number of trace log files to retain before deleting the oldest file.
Rollover File Size (MB)	The maximum size of the trace log file, in megabytes, before the file is rolled over to another historical file.
Error Log File Settings	Error-level logging.
File Name	The name of the error log file. For example, ${SERVER_LOG_ROOT}/SystemErr.log
Maximum number of historical files	The maximum number of error log files to retain before deleting the oldest file.
Rollover File Size (MB)	The maximum size of the error log file, in megabytes, before the file is rolled over to another historical file.
System Log File Settings	System-level logging.
File Name	The name of the system log file. For example, ${SERVER_LOG_ROOT}/SystemOut.log
Maximum number of historical files	The maximum number of system log files to keep before deleting the oldest file.
Rollover File Size (MB)	The maximum size of the system log file, in megabytes, before the file is rolled over to another historical file.
Service Log File Settings	Service-level logging.
File Name	The name of the service log file. For example, ${SERVER_LOG_ROOT}/activity.log

Name	Description
Rollover File Size (MB)	The maximum size of the service log file, in megabytes, before the file is rolled over to another historical file.
Save	Saves the current settings on the page.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.

Related topics:

Logging on page 159

Configuring logging on page 160

JDBC field descriptions

Name	Description
Database Name	The name or identifier assigned to the Avaya one-X® Client Enablement Services database.
Max Connections	The maximum number of connections to the database that you can create in this connection pool. Once you reach this number, you cannot create new connections and you must wait until a connection currently in use is returned to the connection pool.
Min Connections	The minimum number of connections to the database that you can create in this connection pool. If the size of the connection pool is at or below this number, existing connections are not discarded.
Connection Timeout	The number of seconds a request for a connection to the database waits when no connections are available in the connection pool and no new connections can be created, because the maximum number of connections has been reached.
Aged Timeout	The time interval, in seconds, after which an idle or unused connection to the database is discarded. When set to 0, active connections

Name	Description
	to the database remain in the pool indefinitely. Set the **Aged Timeout** parameter higher than the **Reap Time** for optimal performance.
Unused Timeout	The time interval, in seconds, after which an idle or unused connection to the database is discarded. Set the **Unused Timeout** parameter higher than the **Reap Time** for optimal performance.
Reap Time	The time interval, in seconds, between connection pool maintenance runs to remove unused connections. The more often this parameter is run, the greater the efficiencies in connection pool management. Set the **Reap Time** parameter less than the values of **Aged Timeout** and **Unused Timeout**.
Save	Saves the current settings on the page.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.

Related topics:

JDBC connector on page 161

Configuring JDBC on page 161

SIP Local field descriptions

Name	Description
Host	The network address (IP address) of the Avaya one-X® Client Enablement Services server used to communicate with Communication Manager. This is a mandatory field.
Port	The port number used by the Client Enablement Services server to communicate with Communication Manager.

Name	Description
	For secure communication using TLS, configure the port to 5061. This is a mandatory field.
Secure Port	When selected, the port is used for secure communication.
Domain	The **Far-end Domain** you specified on Communication Manager must match the SIP Local **Domain** field value. This is a mandatory field.

Mobile application field descriptions

Name	Description
Url	Location from where the user can download the software update. In a non-HTTP server configuration, the URL is the Client Enablement Services server address. In a HTTP server configuration, the URL is the HTTP server address. This is a mandatory field.
Port	Port number that the application download site uses for the communication. Either in a HTTP server configuration or in a non-HTTP server configuration, this port is 443. However, users can modify the port through the IBM console or by editing the `httpd.conf` file in the HTTP server. This is a mandatory field.
Mobile application filename	Name of the package (zip file) that contains the mobile application binaries and mobile application properties that the administrator uploads into the system.
Manufacturer	Manufacturer of the mobile for which the software update is available.
Model	Model of the mobile for which the software update is available.
Platform name	Name of the platform for which the software update is available. For example, Symbian, Windows Mobile, and so on. This is a mandatory field.

Name	Description
Platform version	Version of the platform for which the software update is available. This is a mandatory field.
Language	Language of the software update. This is a mandatory field.
Type	Type of download. For example, OTA (over the air), App Store, Desktop, and so on.
Product name	Name of the product for which the software update is available. This is a mandatory field.
Product version	Version of the product for which the software update is available. This is a mandatory field.
Release status	Release status of the software update. If the status is **Active**, users can view and download the software update. If the status is **Inactive**, users cannot view the software update. At a time, only one release can be active for a particular manufacturer and model. This is a mandatory field.
Platform features	Feature of the platform for which the software update is available. For example, Standard, Professional, and so on.
Release Notes	Release notes for the software update.
Binary reference	Path where the system stores the binary files.

SMS domains field descriptions

Name	Description
Sms domain	SMS domain of the mobile telephony service provider.
Country	Country for the SMS domain. This is a mandatory field.
Carrier	Mobile telephony service provider.
Region	The geographical area of the mobile communication. This is carrier specific.

Name	Description
Email domain	E-mail domain of the mobile telephony service provider.
Data source	The entity in the system which creates the SMS domain. The options are **Admin** and **Public**. Select **Admin** for an SMS domain data created by an administrator. Select **Public** for an SMS domain data whose source is wikipedia.

Notification service field descriptions

Name	Description
Type	Type of the notification service.
Version	Version of the notification service.
Handle	The unique name assigned to the notification service by the administrator. This is a mandatory field.
Description	A short description of the notification service.
Enabled	Enables the notification service for the system.
TLS Enabled	Adds an extra layer of transport level security to all notifications that are sent to the SMTP server.
Mail Domain	Domain of the mail server used to send notifications. This is a mandatory field.
Max Transport Pool Size	The maximum number of transport connections that can be established with the SMTP server for sending notifications. You can use this to save the SMTP server from getting overloaded with the number of transports being created through the Client Enablement Services server.
Max Queue Size	The maximum number of notifications that can be in the queue.

Name	Description
Retry Connect Period	The maximum period of time (in minutes) the server tries to connect to the client in case of a connection failure. All new notifications are in a pending state during this period.
Monitor: Status	Monitor status is **Enabled** when the notification service is working properly. Monitor status is **Error** when the notification service has some error.
Monitor: Exception	Indicates the reason for the notification service error.
Refresh	Refreshes the monitor status.
Host	IP address of the SMTP server. This is a mandatory field.
Port	The port number used by the notification service to access the SMTP server. This is a mandatory field.
Login ID	The Log-in ID of a valid mail server user account, which has mail send privileges. If you have configured the SMTP server for an anonymous bind, then enter dummy values in the **Login ID** and **Password** fields. This is a mandatory field.
Password	The password to log in to the SMTP server. This is a mandatory field.
Confirm	Verification of the password used to log in to the SMTP server. This is a mandatory field.
TLS configuration	For the SSL supported SMTP provider server connection, import a server certificate. You can upload a certificate file with .cer or.crt extension. When you upload the file, the system validates the file type and the expiry of the certificate date.
Browse	Use to browse the certificate file.
Upload	Use to upload the certificate file.
Save	Saves the new notification service or changes made to the existing notification service.
Reset	Restores the form back to the default or blank values.

Name	Description
Cancel	Exits the page without making any additions or changes.

Chapter 7: Monitors

Monitor services

The Monitor Services feature displays run-time information for Telephony, Modular Messaging, and Conferencing services and associated servers on Avaya one-X® Client Enablement Services.

Note:

If you are an **Auditor**, the **Monitor** tab is not available.

The information includes the following:

- Name of the service
- Type of service
- Version number of the service
- Current state of the service
- Date and time the service started
- Run-time of the service
- Number of client connections to the service
- Number of requests received by the service
- Number of failed requests to the service
- Number of requests that timed out on the service
- Number of outstanding requests to the service

Important:

Always start, stop, or restart any Avaya service using the corresponding Monitors page only. Using any other tool, such as IBM console, to start, stop, or restart a service is not supported.

Related topics:

Monitoring Telephony services on page 186
Monitoring Voice Messaging services on page 186
Monitoring Conferencing services on page 187

Monitoring Telephony services

Procedure

1. Click the **Monitors** tab.

   Note:

   If you are an **Auditor**, you are denied access to this page. Click the back button of the browser to return to the previous page.

2. In the left pane, select **Telephony**.
   The SIP Service displays the connectivity between Communication Manager and Session Manager for SIP link. For more information, see Monitor field descriptions on page 190.

   Note:

   Ignore the request counts for the **CM Service** for telephony. In this release, no server is supported for this service.

3. You can perform the following actions on the **Telephony** services.
   - Click **Stop** to stop the services.
   - Click **Start** to start up the services.
   - Click **Restart** to stop and restart the services.

4. You can also perform the following actions on each **Telephony** server.
   - Click **Suspend** to stop the connection to the server.
   - Click **Resume** to reconnect to the server.

Monitoring Voice Messaging services

Procedure

1. Click the **Monitors** tab.

Note:

If you are an **Auditor**, you are denied access to this page. Click the back button of the browser to return to the previous page.

2. In the left pane, select **Voice Messaging**.
   The Monitor Voice Messaging Services page displays the current status of the **Voice Messaging** services on Avaya one-X® Client Enablement Services. For more information, see Monitor field descriptions on page 190.
3. You can perform the following actions on the **Voice Messaging** services.
   - Click **Stop** to stop the services.
   - Click **Start** to start up the services.
   - Click **Restart** to stop and restart the services.
4. You can also perform the following actions on each **Voice Messaging** server.
   - Click **Suspend** to stop the connection to the server.
   - Click **Resume** to reconnect to the server.

Monitoring Conferencing services

Procedure

1. Click the **Monitors** tab.

Note:

If you are an **Auditor**, you are denied access to this page. Click the back button of the browser to return to the previous page.

2. In the left pane, select **Conferencing**.
   The Monitor Conferencing Services page displays the current run-time status for the services on Avaya one-X® Client Enablement Services. For more information, see Monitor field descriptions on page 190.
3. You can perform the following actions on the **Conferencing** services.
   - Click **Stop** to stop the services.
   - Click **Start** to start up the services.
   - Click **Restart** to stop and restart the services.
4. You can also perform the following actions on each **Conferencing** server.
   - Click **Suspend** to stop the connection to the server.

- Click **Resume** to reconnect to the server.

Monitoring Presence services

Procedure

1. Click the **Monitors** tab.

   Note:

   If you are an **Auditor**, you are denied access to this page. Click the back button of the browser to return to the previous page.

2. In the left pane, select **Presence**.
   The Monitor Presence Services page displays the current run-time status for the services on Avaya one-X® Client Enablement Services. For more information, see Monitor field descriptions on page 190.

3. You can perform the following actions on the **Presence** services.

   - Click **Stop** to shutdown the services.
   - Click **Start** to start up the services.
   - Click **Restart** to stop and restart the services.

4. You can also perform the following actions on each **Presence** server.

   - Click **Suspend** to stop the connection to the server.
   - Click **Resume** to reconnect to the server.

Monitoring Audio Transcoding services

Procedure

1. Click the **Monitors** tab.

   Note:

   If you are an **Auditor**, you are denied access to this page. Click the back button of the browser to return to the previous page.

2. In the left pane, select **Audio Transcoding**.

The Monitor Audio Transcoding Services page displays the current status of the **Audio Transcoding** services on Avaya one-X® Client Enablement Services. For more information, see Monitor field descriptions on page 190.

3. You can perform the following actions on the **Audio Transcoding** services:
    - Click **Stop** to stop the services.
    - Click **Start** to start up the services.
    - Click **Restart** to stop and restart the services.
4. You can also perform the following actions on the Audio Transcoding server:
    - Click **Suspend** to stop the connection to the server.
    - Click **Resume** to reconnect to the server.

Monitoring Handset services

Procedure

1. Click the **Monitors** tab.

    Note:

    If you are an **Auditor**, you are denied access to this page. Click the back button of the browser to return to the previous page.
2. In the left pane, select **Handset**.
    The Monitor Non Adapter Services page displays the current status of the **Handset** services on Avaya one-X® Client Enablement Services. For more information, see Monitor field descriptions on page 190.
3. You can perform the following actions on the **Handset** services:
    - Click **Stop** to stop the services.
    - Click **Start** to start up the services.
    - Click **Restart** to stop and restart the services.

Monitoring other services

About this task

Use the following procedure to monitor other services:

- **User Assistant**
- **Client Portal**
- **Downloads**
- **Online Help**

Procedure

1. Click the **Monitors** tab.

   Note:

   If you are an **Auditor**, you are denied access to this page. Click the back button of the browser to return to the previous page.

2. In the left pane, select **Other Services**.
   The Monitor Non Adapter Services page displays the current status of the **User Assistant** , **Client Portal**, **Downloads**, and **Online Help** services on Avaya one-X® Client Enablement Services. For more information, see Monitor field descriptions on page 190.

3. You can perform the following actions for any of the services:

   - Click **Stop** to stop the services.
   - Click **Start** to start up the services.
   - Click **Restart** to stop and restart the services.

Monitor field descriptions

The Avaya one-X® Client Enablement Services Monitor feature displays the following fields for each of the supported services.

Name	Description
Service	The name assigned to the monitored service. • **CM Service** or **SipService** for Telephony • **MM Service** for **Messaging** • **MX Service** for **Conferencing** • **Presence Service** for **Presence** • **Audio Transcoding Service** for **Audio Transcoding** • **Handset Service** for **Handset**

Name	Description
	• **User Assistant Service** for **User Assistant** • **Client Portal Service** for **Portal Client** • **Downloads Service** for **Download** • **Online Help Service** for **Online Help**
Type	The type of monitored service. • **telephony** or **siptelephony** • **voicemessaging** • **conferencecontrol** • **presence** • **audiotranscoding** • **handsetservice** • **userassistant**
Version	The version number of the monitored service.
State	The current state of the monitored service as **Available** or **Unavailable**.
EAR Name	The name of the deployment EAR file of the monitored service. • **1X_HandsetServices** for **Handset** • **1X_UserAssistant** for **User Assistant** • **1X_Client_Portal** for **Client Portal** • **1X_Downloads** for **Downloads** • **1X_Online_Help** for **Online Help**
Start Time	The date and time of day that the monitored service was last started.
Up Time	The period of time in minutes, seconds, and milliseconds that the monitored services has been running.
Client Connections	The number of clients currently connected to the monitored service.
Request Counts	The number of requests received for the monitored service and the number of failed requests.

Name	Description
	Also displays the number of outstanding timed out requests on the **Admin**, **Client**, and **System** level for the monitored service.
Actions	The message describing any action required for the monitored service and provides the following buttons to perform that action. • **Start** • **Stop** • **Restart**
Servers	Displays the following information for the server that is delivering the monitored service: • **Handle**. The name assigned to the server • **Type**. The type of server, such as Telephony, Voice Messaging, or Conferencing. • **Version**. The version number of the server, such as CM 6.0. • **State**. The current running state of the server, such as connected. - Connected. Adapter is connected with the server. - Started. Adapter service is already started. - Idle. Adapter is not in use. - Starting. Adapter is starting state. - Suspended. Adapter is in suspended state. - Down. Adapter is down and cannot connect. • **Start Time**. The time when the server was started. • **Up Time**. The period of time the server has been running. • **Actions**. Buttons that suspend or resume running of the server.

Chapter 8: Administration Command Line Client

Overview

The Administration Command Line Client commands are an alternative to the administration tasks you can perform using the Avaya one-X® Client Enablement Services administration application.

These commands are useful when you have to do bulk administration such as creating many users at a time or when the administration application is unavailable.

Prerequisite settings on Linux

Before you begin

Java must be installed on the computer.

About this task

To run the command-line interface (CLI) commands, you must set up the CLI client.

Note:

You must perform the following procedure only once before carrying out any other procedure related to CLI commands.

Procedure

1. Go to `/opt/avaya/1xp` directory using the command **`cd /opt/avaya/1xp`**.
2. Run the following command to untar the files:
   a. **`chmod +x 1XP_Admin_CLI_Client.tar`**
   b. **`tar –xvf 1XP_Admin_CLI_Client.tar`**
3. Edit the `connection-store.properties` file using the command **`vi connection-store.properties`**

4. Change the following values in the `connection-store.properties` file as explained below:

    - username=<admin_user_name of the Client Enablement Services system. This is not the Linux admin of the Client Enablement Services template.>
    - password=<admin_pasword of the Client Enablement Services system. This is not the Linux password of the Linux admin of the Client Enablement Services template.>
    - host=<IP of the Client Enablement Services server>
    - secure=<true>
    - port=<9443>

    For example:

    - username=craft
    - password=Avaya123
    - host=192.168.2.24
    - secure=true
    - port=9443

    In this example, 192.168.2.24 is the IP address of the Client Enablement Services server.

Related topics:

Importing user data to the Avaya one-X Client Enablement Services 6.1 server on page 218
Exporting user data from the Avaya one-X Client Enablement Services 6.1 source server on page 220
Importing user data to the Avaya one-X Client Enablement Services 6.1 target server on page 221
Importing dial plan data to the Avaya one-X Client Enablement Services 6.1 server on page 226
Migrating dial plan data from the Client Enablement Services 6.1 server to another Client Enablement Services 6.1 server on page 227

Running CLI commands on a Linux system

About this task

Use the command prompt to run the CLI commands. In the command prompt, run the shell script for the CLI commands, and then add the command for the required action. For example, to import users, perform following steps.

Procedure

1. Go to the `/opt/avaya/1xp` directory using the command: **`cd /opt/avaya/1xp`**
2. In the command prompt, type `./1xpAdmin.sh import users -u /opt/avaya/1xp/<`*`dataexportfilename.csv`*`> -v 6.1`.

   In the above command:

   - `1xpAdmin.sh` is the shell script for running CLI commands. This script is located in the folder where you have unzipped the `1X_Admin_CLI_Client.tar` file.
   - `/opt/avaya/1xp/<`*`dataexportfilename.csv`*`>` is the location of the file on the server from which you import users.
   - <*dataexportfilename.csv*> is the file name of the file that contains user data you want to import.
   - 6.1 is the version of the Client Enablement Services system.
3. Press Enter.
   If the operation is successful, the system displays the message: `File to import is /opt/avaya/1xp/<`*`dataexportfilename.csv`*`>. Operation completed successfully`.

   If the operation is unsuccessful, the system displays a failure message. Information about the operation is available in the log file `acp_admin_cli.log`. By default, this log file is created in the `/opt/IBM/WebSphere/AppServer70/profiles/default/logs/acp_admin_cli.log` directory.

Related topics:

Administration Command Line Client overview on page 14

Running CLI commands on a Windows system on page 196

Prerequisite settings on Windows

About this task

On your Windows 2000 or Windows XP machine, make following changes for Java installation and environment variable settings.

Procedure

1. Right-click **My Computer** and select **Properties**.
2. In the **Advanced** tab, click **Environment variables**.
3. In the **System variables** section, select the **Path variable** and click **Edit**.
4. In the **Edit System variable** window, change the **Variable** value to the path of the Java executable.
   For example, if you have installed Java in `c:\jdk` and your Variable value is currently set to `C:\WINDOWS\SYSTEM32`, then change the Variable value to `C:\WINDOWS\SYSTEM32;c:\jdk\bin`.
5. Click **Ok** to close all the windows.

Result

When you open a new command prompt, it reflects the changes you made and you can run java programs using the command **`java`**.

Note:

If you have installed the JDK, then you can compile the java code using **`javac`**.

Running CLI commands on a Windows system

About this task

Use the command prompt to run the CLI commands. In the command prompt, run the `1xpAdmin.cmd` file for the CLI commands, and then add the command for the required action. For example, to import users perform following steps.

Procedure

1. Copy the `1X_Admin_CLI_Client.tar` file from the Avaya one-X® Client Enablement Services server to the windows machine using WINSCP.
2. Unzip the `1xp_admin_CLI_Client.tar` file.

3. Open the `connection-store.properties` file to edit the file.
4. Change the following values in the `connection-store.properties` file:

    - username=<admin_user_name of the Client Enablement Services system. This is not the Linux admin of the Client Enablement Services template.>
    - password=<admin_pasword of the Client Enablement Services system. This is not the Linux password of the Linux admin of the Client Enablement Services template.>
    - host=<IP of the Client Enablement Services server>
    - secure=<true>
    - port=<9443>

    For example:

    - username=craft
    - password=Avaya123
    - host=192.168.2.24
    - secure=true
    - port=9443

    In this example, 192.168.2.24 is the IP address of the Client Enablement Services server.
5. Change the directory to the location where you copied the `1X_Admin_CLI_Client.tar` file.
6. In the command prompt, type `1xpAdmin.cmd import users -u` *`<dataexportfilename.csv>`* `-v 6.1`.

    In the above command:

    - `1xpAdmin.cmd` is the command file for running CLI commands. This file is located in the folder where you have unzipped the `1X_Admin_CLI_Client.tar` file.
    - *<dataexportfilename.csv>* is the file name of the file that contains user data you want to import.
    - 6.1 is the version of the Client Enablement Services server.
7. Press Enter.
    If the operation is successful, the system displays the following message: `File to import is` *`<dataexportfilename.csv>`*`. Operation completed successfully.`

    If the operation is unsuccessful, the system displays a warning, or failure message. Information about the operation is available in the log file, `acp_admin_cli.log`.

By default, this log file is created in the directory in where you have unzipped the `1x_Admin_CLI_Client.tar` file.

Related topics:

Administration Command Line Client overview on page 14

Running CLI commands on a Linux system on page 195

Admin CLI Commands

Import users

Use the `import users` command to import multiple user records from an Excel or CSV file to the Client Enablement Services database. Run this command in connection with the `export users` command to import users to the database after a database back up, to move users from one database to another, to use the user data on a test system, and so on.

Related topics:

Creating user files on page 198

Creating user files

About this task

To import users, you can either use a CSV file or an Excel file you have exported from an Avaya one-X® Client Enablement Services server or you can create a new CSV or Excel file.

- If you want to import users using a .xls or .csv file generated from the `export users` command, use one of the following procedures as applicable:
    - See User data migration from the Avaya one-X Portal 5.2 server to the Avaya one-X® Client Enablement Services 6.1 server on page 217.
    - See User data migration from one Avaya one-X® Client Enablement Services 6.1 server to another Avaya one-X® Client Enablement Services 6.1 server on page 220.
    - See Migration from the Avaya one-X Mobile 5.2 server to the Avaya one-X® Client Enablement Services 6.1 server on page 222.
- If you want to import users using a new file, you can create a user file before importing users to the Client Enablement Services database. The `import users` and `export users` commands support Excel and CSV formats for the user file. Perform the following steps:

You can create an Excel file to import user data, but you must ensure that the Excel file contains all columns that are present in the Excel file when you export data from the Client Enablement Services server. If one or more columns are missing in the excel file you create, the import procedure fails. Alternatively, you can export the user data from the Client Enablement Services server, and use this file as the template file to import user data.

Procedure

1. Provision a user on the Client Enablement Services administration application and export the user data of this user.
   The user data is exported as an Excel file, and you must use this file as a template to enter information of other users and import user data.

   `/opt/avaya/1xp/<dataexportfilename.csv>` is the default location of the excel file.

   For more information, see Exporting user data from the Avaya one-X Client Enablement Services 6.1 source server on page 220.
2. Enter user information in the appropriate fields in the file.
3. Use the **`import users`** command to import users.

   For more information, see Importing user data to the Avaya one-X Client Enablement Services 6.1 target server on page 221.

Export users

Use the `export users` command to export multiple user records from the Avaya one-X® Client Enablement Services database to an Excel or CSV file. Run this command to export user data during a new Avaya one-X® Client Enablement Services installation and then use the exported Excel or CSV file to import user data to the new system.

Note:

The Administration Command Line Interface supports only bulk export and import of user data. At present, Administration Command Line Interface does not support selective user data export or import.

Related topics:

User data migration from one Avaya one-X® Client Enablement Services 6.1 server to another Avaya one-X® Client Enablement Services 6.1 server on page 220

Provisioned users list

Provisioned users are in the Avaya one-X® Client Enablement Services user group of the Active Directory and reside in the Client Enablement Services database. You can list the users who are provisioned for Client Enablement Services.

Provision user

Use the `provision users` command to put users in the Avaya one-X® Client Enablement Services user group of the Active Directory and into the Client Enablement Services database. Once these users are in the Client Enablement Services database, they are provisioned for Client Enablement Services.

List unprovisioned users

Use the `listUnprovisioned users` command to display a list of those users who are not provisioned for Avaya one-X® Client Enablement Services. Unprovisioned users are in the Client Enablement Services user group of the Active Directory but have not been provisioned and do not reside in the Client Enablement Services database.

Unprovision user

Use the `unprovision users` command to remove users from the Avaya one-X® Client Enablement Services user group and the Client Enablement Services database. Once these users are removed from the Client Enablement Services database, they are unprovisioned from Client Enablement Services.

Assign a group to a user

Use the `assignGroup user` command to assign a group to a user who is provisioned for Avaya one-X® Client Enablement Services. Provisioned users must be in the Client Enablement Services user group of the Active Directory and reside in the Client Enablement Services database.

Create a user resource

Use `create UserResource` commands to assign resources to provisioned users on Avaya one-X® Client Enablement Services. For users to access telephony, messaging, personal contact, or presence on Client Enablement Services, you must create the corresponding resource for those users.

You can assign the following resources to Client Enablement Services users:

- Telephony
- Messaging
- Presence
- Personal Contact

Update user resource

Use the `update UserResource` commands to update the resources that are assigned to provisioned users on Avaya one-X® Client Enablement Services. For users to access telephony, messaging, personal contact, or presence on Client Enablement Services, you must create the corresponding resource for those users. You must update these resources for any change.

Remove user resource

Use `remove UserResource` commands to delete resources that are assigned to provisioned users on Avaya one-X® Client Enablement Services.

You can remove the following resources assigned to the user:

- Telephony
- Messaging
- Presence
- Personal Contact

Terminate a user session

Use the `terminate user` command to end the current session of a provisioned user on Avaya one-X® Client Enablement Services.

Manage servers

Use the `create server`, `update server`, and `delete server` CLI commands to create, update, and delete following servers:

- Telephony
- Voice Messaging
- Conferencing
- Presence

Create, update, and delete Group profile

A Group profile is a collection of properties that are applied to users who are members of the group. Use the `create groupProfile`, `update groupProfile`, and `delete groupProfile` commands to create, update, and delete Group profiles.

Update System profile

System profile is a collection of properties that are applied to groups that are members of the system. Use the `update systemProfile` command to update the System profile.

Create, update, and delete SNMP destination

Use the `create snmpdestination`, `update snmpdestination`, and `delete snmpdestination` commands to create, update, and delete SNMP destinations. SNMP destinations are devices to which you can send specified traps such as event notifications. On Avaya one-X® Client Enablement Services, these devices can either be the Avaya Services Security Gateway (SSG) or industry standard Network Monitoring Software (NMS) such as HP Openview or IBM Tivoli.

Monitor services

To display the current runtime status for the services, use the `list services`, `start service`, `stop service`, and `restart service` commands to list, start, stop, and restart the following services:

- Telephony
- Voice Messaging
- Conferencing
- Presence

Monitor servers

Use the `suspend server` and `resume server` commands to monitor and display the status of the servers running on the following Avaya one-X® Client Enablement Services registered services.

- For the messaging service, displays the status of Voice Messaging servers.
- For the Communication Manager Service, displays the status of Telephony servers.
- For the presence service, displays the status of Presence Services servers.
- For the Conferencing Service, displays the status of Conferencing servers.

These commands display information such as connection start time, connection state, connection up time, server name, and server ID for these Client Enablement Services servers.

Migrate server

Use the migrate server commands to upgrade servers configured to work with Avaya one-X® Client Enablement Services from one version to another version. The CLI client supports the server migration functionality.

`list Migration server` command and `migrate server` command are the two CLI commands that support the migration of provider servers to new versions.

list Migration server command

```
list Migration server [ ] -- newVersion -n | --handle -h
```

In this command:

- -h is the handle that identifies existing server adapter.
- -n specifies the new version to which the server is migrated.

List migration shows:

- A list of current property values assigned to the server handle.
- A list of property values assigned to the server handle that is going to be removed.
- A list of new property values that is going to be assigned to the server handle.

migrate server command

```
migrate server [ --paramNames -m | --paramValues -v ] -- newVersion -n | --
handle -h
```

In this command:

- -h is the handle that identifies existing server adapter.
- -n specifies the new version to which the server is migrated.

For paramNames and paramValues that are not specified in the command, the migration tool uses the old values assigned to the server handle.

Note:

You can verify the migration for the respective servers and users from the **Servers** and **Users** tabs of the Web Administration client.

Add Encryption Keys

Perform the following steps before you use the add encryption keys command:

1. Create a file with the extension .keys.
2. Enter vi sample.keys values for keys in this file.

   The file should contain pairs of key name and key value as per the following format:

   `keyname:<yourKeyName> keyvalue:<yourKeyValue>`
3. Save the file.

Use the **`add key -f <the keys file name>`** command to add encryption keys to the `cryptoKey` table in the Client Enablement Services database.

Specify the absolute path of the .keys file you created while executing the add encryption keys command.

Associate Key To Column

Use the **`associate columntokey -o oldkeyName -n NewKeyName -c Column name`** command to associate the keys added to Client Enablement Services through the **`add key -f <the keys filename>`** command to the specified column of the database table.

These columns contain passwords for extension banks, log-in name for network addresses, passwords for network addresses, PIN for user resources, passwords for user resources, and user device settings. Adding the key to a column, encrypts the data in that column. You can use one key for association to all the columns in the table or use one key for each of the columns in the database table. The database table contains five columns that can be encrypted.

The oldkeyName is used in case there is a change in the key name, whose new value is newKeyName.

Column name is the name of the column whose values you want to encrypt. For a column that contains

- passwords for extension banks, enter EXTN_BANK_PWD
- log-in name for network addresses, enter NETWORK_ADDR_PWD
- passwords for network addresses, enter NETWORK_ADDR_LOGON
- pin for user resources, enter USER_RES_PWD
- passwords for user resources, enter USER_RES_PIN
- user device settings, enter USER_DEV_SETTING_MISC1 or USER_DEV_SETTING_MISC2

Run Key Migration

Use the **`migrate key`** command to encrypt the values of the columns used in the **`associate columntokey`** command. This is the third step in the encryption key process after adding the encryption keys and associating the keys these columns in the database table. This script does not require additional parameters.

Example

The content of the file temp.keys can be: `keyname:testKey`
`keyvalue:ABCDEFG123456789`

Use these commands for user resource password encryption.

```
./1xpAdmin.sh add key -f /tmp/temp.keys
```

```
./1xpAdmin.sh associate columntokey -n testKey -c USER_RES_PWD
```

```
./1xpAdmin.sh migrate key
```

CLI commands for administrative tasks

Each command consists of the **`command resource [ optional_arguments ] required_arguments`**. You should write the optional arguments also, but you must write the required arguments for each command.

Action	Command	Example
Creating a telephony server	`create server --telephony -t [ | --coreServerDescription -d | --coreServerEnabled -e | --dialPlan -r | ] --handle -h | --serverType -y | --serverVersion -v | --serverName -s | --telServerName -n | --telServerMovEnabledCode -o | --telServerMovDisabledCode -f | --telServerMovModNumberCode -q`	create server –t -d <Description of the core server> -e <Enable the core server> -r <Dial plan> -h <handle> -y <type of server> -v <version of the server> -s <name of the server> -n <name of the telephony server> -o <Extension to cellular feature enable code> -f <Extension to cellular feature disable code> -q <Extension to cellular feature modify code>
Creating a voice messaging server	`create server --voiceMessaging -m [--coreServerDescription -d | --coreServerEnabled -e | --numConnections -nc | --maxNumConnection -mc | --connectionsincrement -ci | --usersperconnection -uc | --workdirectory -wd | --timeToLive -tl] --handle -h | --serverType -y | --serverVersion -v | --mailDomainName -md | --imapName -in | --imapPort -ip | --imapLoginID -il | --imapPassword -iw | --`	create server -m –d<description of the core server> -e <enable the core server> -nc <initial number of server connection> -mc <maximum number of server connection> -ci <client connections increment> -uc < users per connection> -wd <temporary directory for the messages> -tl <time to live> -h <handle> -y <server type> -v <version of the server> -md <domain name of the mail server> -in <IMAP name> -ip <IMAP port> -il <IMAP login ID> -iw <IMAP password> -is <secure port for IMAP> -sn <SMTP name> -sp <SMTP port> -sl < SMTP login ID> -sw <SMTP password> -ss <secure SMTP> -ln <LDAP

Action	Command	Example
	`imapSecure -is | --smtpName -sn | --smtpPort -sp | --smtpLoginID -sl | --smtpPassword -sw | --smtpSecure -ss | --ldapName -ln | --ldapPort -lp | --ldapLoginID -ll | --ldapPassword -lw | --ldapSecure -ls`	name> -lp <LDAP port> -ll <LDAP login ID> -lw <LDAP password> -ls <secure LDAP>
Creating a conference server	`create server --conference -c [--bcapiLoggerDirectory -b | --coreServerDescription -d | --coreServerEnabled -e | --dialPlan -r] --handle -h | --serverType -y | --serverVersion -v | --bcapiHost -bh | --bcapiLoginID -bl | --bcapiPassword -bp | --bcapiSecondLoginID -sl | --bcapiSecondPassword -sp | --crsHost -ch | --crsPort -cp | --crsLoginID -cl | --crsPassword -cw`	create server -c –b <BCAPI Logger Directory> -d <description of the core server> -e <enable the core server> -r <dial plan> -h <handle> -y <server type> -v <version of the server> -bh <BCAPI host> -bl <BCAPI login ID> -bp <BCAPI password> -sl < BCAPI second login ID> -sp <BCAPI second password> -ch <CRS host> -cp <CRS port> -cl <CRS login ID> -cw <CRS password>
Creating a presence server	`create server --presence -p [ --serverType -y | --serverVersion -v | --coreServerDescription -d | --coreServerEnabled -e | --ipsPublish -ip | --lpsConsumer -lc | --lpsSupplier -lp ] --handle -h | --umsURL -u | --ipsHost -ih | --ipsPort -ir | --umsHost -uh | --umsPort -up | --`	create server -p -y <server type> -v <version of the server> -d <description of the core server> -e <enable the core server> -ip <publish to port> -lc <consumer port> -lp <supplier port> -h <handle> -u <UMS URL> -ih <IPS host> -ir <IPS port> -uh <UMS host> -up <UMS port> -ul <UMS login ID> -uw <UMS password>

Action	Command	Example
	umsLoginID -ul | --umsPassword -uw	
Updating a telephony server	update server --telephony -t [| --serverType -y | --serverVersion -v | --serverName -s | --coreServerDescription -d | --coreServerEnabled -e | --telServerName -n | --telServerMovEnabledCode -o | --telServerMovDisabledCode -f | --telServerMovModNumberCode -q | --dialPlan -r] --handle -h	update server -t -y <server type> -v <server version> -s <server name> -d <description of the core server> -e <enable the core server> -n <name of the telephony server> -o <Extension to cellular feature enable code> -f <Extension to cellular feature disable code> -q <Extension to cellular feature modify code> -r <dial plan> -h <handle>
Updating a voice messaging server	update server --voiceMessaging -m [--serverType -y | --serverVersion -v | --coreServerDescription -d | --coreServerEnabled -e | --numConnections -nc | --maxNumConnection -mc | --connectionsincrement -ci | --usersperconnection -uc | --workdirectory -wd | --timeToLive -tl | --mailDomainName -md | --imapName -in | --imapPort -ip | --imapLoginID -il | --imapPassword -iw | --imapSecure -is | --smtpName -sn | --smtpPort -sp | --smtpLoginID -sl | --smtpPassword -sw | --smtpSecure -ss | --ldapName -ln | --	update server -m -y <server type> -v <version of the server> –d<description of the core server> -e <enable the core server> -nc <initial number of server connection> -mc <maximum number of server connection> -ci <client connections increment> -uc <users per connection> -tl <time to live> -md <domain name of the mail server> -wd <temporary directory for the messages> -in <IMAP name> -ip <IMAP port> -il <IMAP login ID> -iw <IMAP password> -is <secure port for IMAP> -sn <SMTP name> -sp <SMTP port> -sl < SMTP login ID> -sw <SMTP password> -ss <secure SMTP> -ln <LDAP name> -lp <LDAP port> -ll <LDAP login ID> -lw <LDAP password> -ls <secure LDAP> -h <handle>

Action	Command	Example
	`ldapPort -lp | --ldapLoginID -ll | --ldapPassword -lw | --ldapSecure -ls ] --handle -h`	
Updating a conference server	`update server --conference -c [--serverType -y | --serverVersion -v | --bcapiLoggerDirectory -b | --coreServerDescription -d | --coreServerEnabled -e | --dialPlan -r | --bcapiHost -bh | --bcapiLoginID -bl | --bcapiPassword -bp | --bcapiSecondLoginID -sl | --bcapiSecondPassword -sp | --crsHost -ch | --crsPort -cp | --crsLoginID -cl | --crsPassword -cw] --handle -h`	update server -c -y <server type> -v <version of the server> –b <BCAPI Logger Directory> -d <description of the core server> -e <enable the core server> -r <dial plan> -bh <BCAPI host> -bl <BCAPI login ID> -bp <BCAPI password> -sl < BCAPI second login ID> -sp <BCAPI second password> -ch <CRS host> -cp <CRS port> -cl <CRS login ID> -cw <CRS password> -h <handle>
Updating a presence server	`update server --presence -p [--serverType -y | --serverVersion -v | --coreServerDescription -d | --coreServerEnabled -e | --ipsPublish -ip | --lpsConsumer -lc | --lpsSupplier -lp | --umsURL -u | --ipsHost -ih | --ipsPort -ir | --umsHost -uh | --umsPort -up | --umsLoginID -ul | --umsPassword -uw] --handle -h`	update server -p -y <server type> -v <version of the server> -d <description of the core server> -e <enable the core server> -ip <publish to port> -lc <consumer port> -lp <supplier port> -u <UMS URL> -ih <IPS host> -ir <IPS port> -uh <UMS host> -up <UMS port> -ul <UMS login ID> -uw <UMS password> -h <handle>
Deleting a telephony server	`delete server --telephony -t --handle -h`	delete server -t -h <handle>

Action	Command	Example
Deleting a voice messaging server	`delete server --voiceMessaging -m --handle -h`	delete server -m -h < handle>
Deleting a conference server	`delete server --conference -c --handle -h`	delete server -c -h <handle>
Deleting a presence server	`delete server --presence -p --handle -h`	delete server -p -h <handle>
Provisioning a user	`provision user [ --prototypeName -p | --group -g | --enabled -e ] --name -n`	provision user -p <prototype user> -g <group profile> -e <enable> -n <name of the user>
Unprovisioning a user	`unprovision user [ ] --name -n`	unprovision user -n <name of the user>
Terminating a user	`terminate user [ ] --name -n`	terminate user –n <name of the user>
Assigning a group to a user	`assignGroup user [ ] --group -g | --name -n`	assignGroup user -g <group profile> -n <name of the user>
Enabling a user	`enable user [ ] --enabled -e | --name -n`	enable user -e <enable> -n <name of the user>
Creating a telephony resource for a user	`create userResource --telephony -t [ --display -d | --address -a | --extension -e | --password -r ] --user -u | --server -s`	create userResource -t -d <display name> -a <display address> -e <phone extension> -r <password> -u <user’s name> -s <telephony server>
Creating a messaging resource for a user	`create userResource --messaging -m [ --display -d | --address -a | --mailbox -e | --password -r | --websubopt -o ] --user -u | --server -s`	create userResource -m -d <display name> -a <display address> -e <mailbox> -r <password to access the mailbox> -o <web subscriber options URL> -u <user name> -s <server>
Creating a presence resource for a user	`create userResource --presence -p [ --display -d | --address -a | --handle -h | --password -r ]`	create userResource -p -d <display name> -a <display address> -h < handle> -r <password> -u <user name> -s <server>

Action	Command	Example
	`--user -u | --server -s`	
Creating a personal contact resource for a user	`create userResource --personalcontact -f [ --display -d | --address -a | --email -e ] --user -u | --server -s`	create userResource -f -d <display name> -a <display address> -e <e-mail of the user> -u <user name> -s <server>
Updating a telephony resource for a user	`update userResource --telephony -t [ --server -s | --display -d | --address -a | --password -r ] --user -u | --extension -e`	update userResource -t -s <server name> -d <display name> -a <display address> -r <password> -u <user name> -e <phone extension>
Updating a conference resource for a user	`update userResource --conference -c [ --server -s | --display -d | --address -a | --pin -n | --moderator -mc | --participant -pc | --bridge -b | --secondary -r | --callme -w ] --user -u`	update userResource -c -s <conference server> -d <display name> -a <display address> -n <pin code> -mc <moderator code> -pc < participant code> -b <bridge number> -r <bridge number backup> -w <enable call me> -u <user name>
Updating a messaging resource for a user	`update userResource --messaging -m [ --display -d | --address -a | --mailbox -e | --password -r | --websubopt -o ] --user -u | --server -s`	update userResource -m -d <display name> -a <display address>-e <mailbox> -r <password to access the mailbox> -o <web subscriber options URL> -u <user name> -s <server>
Updating a presence resource for a user	`update userResource --presence -p [ --server -s | --display -d | --address -a | --password -r ] --user -u`	update userResource -p -s <server> -d <display name> -a <display address> -r <password> -u <user name>
Updating a personal contact resource for a user	`update userResource --personalcontact -f [ --server -s | --display -d | --address -a ] --user -u | --email -e`	update userResource -f -s <server> -d <display name> -a <display address> -u <user name> -e <e-mail of the user>

Action	Command	Example
Removing a telephony resource for a user	`remove userResource --telephony -t --user -u | --extension -e`	remove userResource -t -u <name of the user> -e <phone extension>
Removing a messaging resource for a user	`remove userResource --messaging -m [ --mailbox -e ] --user -u | --server -s`	remove userResource -m –e <mailbox number> -u <name of the user> -s <server name>
Removing a presence resource for a user	`remove userResource --presence -p --user -u`	remove userResource -p -u <name of the user>
Removing a personal contact resource for a user	`remove userResource --personalcontact -f --user -u | --email -e`	remove userResource -f -u <name of the user> -e <e-mail of the user>
Listing users	`list users [ --searchBy -s | --group -g | --server -r | --pattern -p ]`	list users -s <search criteria> -g <from the specific group name> -r <from the specific server> -p <pattern>
Listing unprovisioned users	`listUnprovisioned users [ --searchBy -s | --pattern -p ]`	list unprovisioned users -s <search criteria> -p <pattern>
Importing users	`import users [ --encrypt -e | --password -p ] --systemVersion -v --userFile -u`	import users –e <if the data should be encrypted> -p <password> -v <version of Client Enablement Services system from which the user file are exported> -u <file name of the user>
Exporting users	`export users [ ] --password -p | --userFile -u`	export users –p <password> -u <file name of the users>
Creating an SNMP destination	`create snmpdestination [ --enabled -e | --deviceType -d | --port -p | --notificationType -nt | --snmpVersion -sv | --userName -un | --securityLevel -sl | --authenticationProtocol -ap | --authenticationPasswor`	create snmpdestination -e <enable the configuration of the SNMP trap> -d <device to which trap are generated> -p <port number for sending the traps> -nt <method of notification> -sv <version of SNMP> -un <user name associated with the destination> -sl <security level assigned> -ap <authentication protocol> -aw <authentication

Action	Command	Example
	`d -aw | --privacyProtocol -pp | --privacyPassword -pw ] --host -h | --handle -hd`	password> -pp <privacy protocol used to encrypt SNMP version 3 messages> -pw <privacy password for encrypting SNMP version 3 messages> -h <IP address of the device used when sending the traps> -hd <handle>
Updating an SNMP destination	`update snmpdestination [ --host -h | --enabled -e | --deviceType -d | --port -p | --notificationType -nt | --snmpVersion -sv | --userName -un | --securityLevel -sl | --authenticationProtocol -ap | --authenticationPassword -aw | --privacyProtocol -pp | --privacyPassword -pw ] --handle -hd`	update snmpdestination -h <IP address of the device used when sending the traps> -e <enable the configuration of the SNMP trap> -d <device to which trap are generated> -p <port number for sending the traps> -nt <method of notification> -sv <version of SNMP> -un <user name associated with the destination> -sl <security level assigned> -ap <authentication protocol> -aw <authentication password> -pp <privacy protocol used to encrypt SNMP version 3 messages> -pw <privacy password for encrypting SNMP version 3 messages> -hd <handle>
Deleting an SNMP destination	`delete snmpdestination [ ] --handle -hd`	delete snmpdestination -hd <handle>
Creating a group profile	`create groupProfile [ --description -d | --extMonitoring -em | --mobility -m | --forwardInbox -fi | --messageFile -mf | --maxFavorites -fn | --accessType -at | --accessLevel -al | --telPresence -tp ] --handle -hd`	create groupProfile -d <description> | - -em <settings for Extension Contact Logging> -m <settings for mobility> -fi <settings for forward voice messages to inbox> -mf <settings for maximum voice messages> -fn <settings for maximum number of favorites> -at <settings for default access type> -al <settings for default access

Action	Command	Example
		level> -tp <settings for tele presence> -hd <handle of group profile>
Updating a group profile	`update groupProfile [ --description -d | --extMonitoring -em | --mobility -m | --forwardInbox -fi | --messageFile -mf | --maxFavorites -fn | --accessType -at | --accessLevel -al | --telPresence -tp ] --handle -hd`	update groupProfile -d <description> | - -em <settings for Extension Contact Logging> -m <settings for mobility> -fi <settings for forward voice messages to inbox> -mf <settings for maximum voice messages> -fn <settings for maximum number of favorites> -at <settings for default access type> -al <settings for default access level> -tp <settings for tele presence> -hd <handle of group profile>
Deleting a group profile	`delete groupProfile [ ] --handle -hd`	Delete groupProfile –hd <handle of group profile>
Updating a system profile	`update systemProfile [ --extMonitoring -em | --mobility -m | --forwardInbox -fi | --messageFile -mf | --maxFavorites -fn | --accessType -at | --accessLevel -al | --telPresence -tp | --disclaimer -di | --disclaimerURL -du | ]`	update systemProfile -em <settings for Extension Contact Logging> -m <settings for mobility> -fi <settings for forward voice messages to inbox> -mf <settings for maximum voice messages> -fn <settings for maximum number of favorites> -at <settings for default access type> -al <settings for default access level> -tp <settings for tele presence> -di <settings for usage disclaimer> -du <settings for disclaimer URL>
Listing telephony services	`list services --telephony -t`	list services –t
Listing voice messages services	`list services --voiceMessages -v`	list services –v
Listing conference services	`list services --conference -c`	list services –c

Action	Command	Example
Listing presence services	`list services --presence -p`	list services –p
Starting a telephony service	`start service --telephony -t --serviceName -sn`	start service –t –sn <name of the service>
Starting a voice messaging service	`start service --voiceMessages -v --serviceName -sn`	start service –v –sn <name of the service>
Starting a conference service	`start service --conference -c --serviceName -sn`	start service –c –sn <name of the service>
Starting a presence service	`start service --presence -p --serviceName -sn`	start service –p –sn <name of the service>
Stopping a telephony service	`stop service --telephony -t --serviceName -sn`	stop service –t –sn <name of the service>
Stopping a voice messaging service	`stop service --voiceMessages -v --serviceName -sn`	stop service –v –sn <name of the service>
Stopping a conference service	`stop service --conference -c --serviceName –sn`	stop service –c –sn <name of the service>
Stopping a presence service	`stop service --presence -p --serviceName -sn`	stop service –p –sn <name of the service>
Restarting a telephony service	`restart service --telephony -t --serviceName -sn`	restart service –t –sn <name of the service>
Restarting a voice messaging service	`restart service --voiceMessages -v --serviceName -sn`	restart service –v –sn <name of the service>
Restarting a conference service	`restart service --conference -c --serviceName -sn`	restart service –c –sn <name of the service>
Restarting a presence service	`restart service --presence -p --serviceName -sn`	restart service –p –sn <name of the service>
Resuming a telephony server	`resume server --telephony -t --`	resume server –t –sn <name of the service> -sr <name of the server>

<table>
<tr><th>Action</th><th>Command</th><th>Example</th></tr>
<tr><td></td><td><code>serviceName -sn | --serverName -sr</code></td><td></td></tr>
<tr><td>Resuming a voice message server</td><td><code>resume server --voiceMessages -v --serviceName -sn | --serverName -sr</code></td><td>resume server –v –sn <name of the service> -sr <name of the server></td></tr>
<tr><td>Resuming a conference server</td><td><code>resume server --conference -c --serviceName -sn | --serverName -sr</code></td><td>resume server –c –sn <name of the service> -sr <name of the server></td></tr>
<tr><td>Resuming a presence server</td><td><code>resume server --presence -p --serviceName -sn | --serverName -sr</code></td><td>resume server –p –sn <name of the service> -sr <name of the server></td></tr>
<tr><td>Suspending a telephony server</td><td><code>suspend server --telephony -t --serviceName -sn | --serverName -sr</code></td><td>suspend server –t –sn <name of the service> -sr <name of the server></td></tr>
<tr><td>Suspending a voice message server</td><td><code>suspend server --voiceMessages -v --serviceName -sn | --serverName -sr</code></td><td>suspend server –v –sn <name of the service> -sr <name of the server></td></tr>
<tr><td>Suspending a conference server</td><td><code>suspend server --conference -c --serviceName -sn | --serverName -sr</code></td><td>suspend server –c –sn <name of the service> -sr <name of the server></td></tr>
<tr><td>Suspending a presence server</td><td><code>suspend server --presence -p --serviceName -sn | --serverName -sr</code></td><td>suspend server –p –sn <name of the service> -sr <name of the server></td></tr>
<tr><td>Listing Migration servers</td><td><code>list Migration server [ ] --newVersion -n | --handle -h</code></td><td>list Migration server –n <version of the new server> -h <handle></td></tr>
<tr><td>Migrating servers</td><td><code>migrate server [--paramNames -m | --paramValues -v] --newVersion -n | --handle -h</code></td><td>migrate server –m<name of the parameters> -v<parameter values> -n <version of the new server> -<handle></td></tr>
<tr><td>Adding encryption keys</td><td>add key -f <the keys filename></td><td>add key -f <the keys filename></td></tr>
<tr><td>Associating keys to column</td><td>associate columntokey -o oldkeyName -n</td><td>associate columntokey -o oldkeyName -n</td></tr>
</table>

Action	Command	Example
	NewKeyName -c Column name	NewKeyName -c Column name
Running key migration	migrate key	migrate key

User data migration

User data migration from the Avaya one-X® Portal 5.2 server to the Avaya one-X® Client Enablement Services 6.1 server

You can migrate users through export-import of user data using the administration CLI tool. The export operation creates a .csv file. The import operation reads the file, processes the data, and provisions users in the database.

Related topics:

Exporting user data from the Avaya one-X Portal 5.2 server on page 217

Importing user data to the Avaya one-X Client Enablement Services 6.1 server on page 218

Exporting user data from the Avaya one-X® Portal 5.2 server

Procedure

1. In the SSH terminal session on the Avaya one-X® Portal 5.2 server, log in as root.
2. Change to the `/opt/avaya/1xp/bin` directory using the command: `cd /opt/avaya/1xp/bin`
3. Convert the CSV file to UNIX format using the command: `dos2unix 1xpAdmin.sh`
4. Export the existing users from the Avaya one-X® Portal 5.2 server using the following command: `./1xpAdmin.sh -u <`*`admin username`*`> -p <`*`admin password`*`> -host <`*`5.2 host ip`*`> -port 8880 -scriptFile ExportUsers.py -userFile /opt/avaya/1xp/bin/<`*`dataexportfilename.csv`*`> -pwd <`*`password for encryption`*`>`
   For example: `./1xpAdmin.sh -u `*`craft`*` -p `*`Avaya123`*` -host `*`192.168.1.38`*` -port 8880 -scriptFile ExportUsers.py -userFile /opt/avaya/1xp/bin/`*`5_2users.csv`*` -pwd `*`avaya`*

In this example, 192.168.1.38 is the IP address of the Avaya one-X® Portal 5.2 server.

> ✱ **Note:**
>
> When you export data from Avaya one-X® Portal 5.2 server to Client Enablement Services 6.1 server, the password is encrypted. The resulting encrypted password should not be more than 32 characters long and you should use only alphabets in the password.

5. Copy the file exported in Step 4 to the Client Enablement Services 6.1 server in the `/opt/avaya/1xp` directory using the command: `scp /opt/avaya/1xp/bin/<`*`dataexportfilename.csv`*`> root@<`*`6.1 host ip`*`>:/opt/avaya/1xp`

   For example: `scp /opt/avaya/1xp/bin/5_2users.csv root@192.168.2.24:/opt/avaya/1xp`

   In this example, 192.168.2.24 is the IP address of the Client Enablement Services 6.1 server.

Importing user data to the Avaya one-X® Client Enablement Services 6.1 server

Before you begin

- You must set up the CLI client on the Client Enablement Services 6.1 before proceeding with the user data migration. For procedure, see Prerequisite settings on Linux on page 193.
- For a successful import of users, ensure that all the users provisioned in Avaya one-X® Portal 5.2 are present in the unprovisioned list of users in Client Enablement Services 6.1. You need to run a full sync first to have enterprise users in the unprovisioned list.
- Ensure that in Client Enablement Services 6.1, the Server Profile names, that is, the Handles for Telephony, Voice Messaging, Conference, and Presence server are same as that in Avaya one-X® Portal 5.2. This refers to the name of each handle, and not the configuration of the handle itself. If there is any change in the handle name, you must modify the exported user data file before importing users from the file. Users whose handles do not match are not imported.

  Note that Client Enablement Services Release 6.1 supports Presence Services Release 6.1. Therefore, you must change the handle of the Presence Services server. To change the handle, copy the CSV file from the Client Enablement Services system to your system, modify the file, and copy the file back to the Client Enablement Services system.

Note:

Before saving the spreadsheet, ensure that the columns containing long strings have the format set to numeric and no decimals. This prevents Excel conversions on data.

- Ensure that the Group Profile names in Client Enablement Services 6.1 are the same as that in Avaya one-X® Portal 5.2. Else, the system does not import the users.

Procedure

1. In the SSH terminal session on the Client Enablement Services 6.1 server, log in as root.
2. Change to the `/opt/IBM/WebSphere/AppServer/java/bin` directory using the command: `cd /opt/IBM/WebSphere/AppServer/java/bin`
3. Copy the `admin_user_file.jar` file from directory `/opt/avaya/1xp/migration` to directory `/opt/IBM/WebSphere/AppServer/java/bin`.
4. Modify the CSV file exported from the Avaya one-X® Portal 5.2 setup to work in the Client Enablement Services 6.1 setup using the command: `./java –jar /opt/IBM/WebSphere/AppServer/java/bin/admin_user_file.jar <`*`absolute path and dataexportfilename.csv`*`>`

   For any file in the Avaya one-X® Portal 5.2 setup, run the above command only once. Ensure that you are logged in as root while running the above command.

   For example: `./java –jar /opt/IBM/WebSphere/AppServer/java/bin/admin_user_file.jar /opt/avaya/1xp/5_2users.csv`
5. Change to the `/opt/avaya/1xp` directory and import the users using the command: `./1xpAdmin.sh import users -u <`*`absolute path and dataexportfilename.csv`*`> -v 5.2 -e true -p <`*`encryption password`*`>`
   For example: `./1xpAdmin.sh import users -u` *`/opt/avaya/1xp/5_2users.csv`* `-v 5.2 -e true -p` *`avaya`*
6. In the Client Enablement Services administration application, verify if all the users are imported correctly. Go to **Users** > **Provisioned Users** page.

   If in the Avaya one-X® Portal 5.2 server, the **Display Name** field value is blank for some provisioned users, but other fields are populated with values, then after the import to Client Enablement Services 6.1, the value of **Display Name** field can be same as the field value of some other field, for example, **Extension** or **Mailbox** or **PinCode**. You can update the **Display Name** value later using the login wizard.

   When you import users, the details of the Presence resource assigned to the user is not imported. Therefore, after you import users, you have to assign Presence resource, Mobile Telephony resource, and Personal Contact resource to each user.

   If the import finishes without any error message, but the users are not imported, check the `connection-store.properties` file.

If the import finishes with an error message such as operation completed with errors, this does not indicate that the import has failed. This is an indicator that some users are not imported because their handles did not match.

Related topics:

Prerequisite settings on Linux on page 193

User data migration from one Avaya one-X® Client Enablement Services 6.1 server to another Avaya one-X® Client Enablement Services 6.1 server

You can migrate user data through export and import of user data using the administration CLI tool. The export operation creates a CSV file. The import operation reads the file, processes the data, and provisions users in the database.

Related topics:

Export users on page 199

Exporting user data from the Avaya one-X Client Enablement Services 6.1 source server on page 220

Importing user data to the Avaya one-X Client Enablement Services 6.1 target server on page 221

Exporting user data from the Avaya one-X® Client Enablement Services 6.1 source server

Before you begin

You must set up the CLI client on the Client Enablement Services 6.1 before proceeding with the user data export procedure. For procedure, see Prerequisite settings on Linux on page 193.

Procedure

1. In the SSH terminal session on the Client Enablement Services 6.1 source server, log in as root.
2. Export users from the Client Enablement Services 6.1 source server using the command:`./1xpAdmin.sh export users –u` *`<dataexportfilename.csv>`* `-p` *`<password for encryption>`*
   For example: `./1xpAdmin.sh export users -u` *`6.1_users.csv`* `-p` *`avaya`*
3. Copy the exported file to the Client Enablement Services 6.1 target server in the `/opt/avaya/1xp` directory using the command: `scp /opt/avaya/1xp/`

`<dataexportfilename.csv> root@<6.1 target server ip>:/opt/avaya/1xp/bin`
For example: `scp /opt/avaya/1xp/6.1_users.csv root@192.168.2.24:/opt/avaya/1xp/bin`

In this example, 192.168.2.24 is the IP address of the Client Enablement Services 6.1 target server.

Related topics:
Prerequisite settings on Linux on page 193

Importing user data to the Avaya one-X® Client Enablement Services 6.1 target server

Before you begin

- You must set up the CLI client on Client Enablement Services 6.1 server before proceeding with the user data import. For procedure, see Prerequisite settings on Linux on page 193.
- For a successful import of users, ensure that all the users provisioned in Client Enablement Services 6.1 source server are present in the unprovisioned list of users in Client Enablement Services 6.1 target server. Perform an enterprise directory synchronization to get the enterprise users in the unprovisioned users list of Client Enablement Services.
- Ensure that in Client Enablement Services 6.1 target server, the Handle for Telephony, Voice Messaging, Conference, and Presence server are same as that in the Client Enablement Services 6.1 source server. This refers to the name of the handle, and not the configuration of the server. Users whose handles do not match are not imported.

  You need to copy the CSV file from the Client Enablement Services system to your system, modify the CSV file, and copy the file back to the Client Enablement Services system.

  Note:

  Before saving the spreadsheet, ensure that the columns containing long strings have the format set to numeric and no decimals. This prevents Excel conversions on data.
- Ensure that the Group Profile names in Client Enablement Services 6.1 target server are the same as that in Client Enablement Services 6.1 source server. Else, the system does not import the users.

Procedure

1. In the SSH terminal session on the Client Enablement Services 6.1 target server, log in as root.
2. Change to the `/opt/avaya/1xp/bin` directory and import the users using the command: `./1xpAdmin.sh import users -u <absolute path and`

```
dataexportfilename.csv> -v 6.1 -e true -p <encryption
password>
```

For example:

```
./1xpAdmin.sh import users -u /opt/avaya/1xp/6.1_users.csv -
v 6.1 -e true -p avaya
```

3. In the Client Enablement Services administration application, verify if all the users are imported correctly. In the administration application, go to **Users** > **Provisioned Users**.
   If the import finishes without any error message, but the users are not imported, check the `connection-store.properties` file.

   If the import finishes with an error message such as operation completed with errors, this does not indicate that the import has failed. This is an indicator that some users are not imported because their handles did not match.

Related topics:

Prerequisite settings on Linux on page 193

Migration from the Avaya one-X® Mobile 5.2 server to the Avaya one-X® Client Enablement Services 6.1 server

Avaya one-X® Mobile server Release 5.2 uses HTTP based protocol for connecting with the Avaya one-X® Mobile client application. In Client Enablement Services Release 6.1, the handset server uses the proprietary communication protocol to connect to the Avaya one-X® Mobile client application Release 6.1. The connection among the Client Enablement Services server, the handset server, and the client application is secured through SSL v3.

For more information about handset server installation, see *Implementing Avaya one-X® Client Enablement Services*.

In Release 6.1, the client application is designed to work with the proprietary protocol. Therefore, these client applications do not work with Avaya one-X® Mobile server Release 5.2. For similar reasons, the Release 5.2 client applications do not work with the Client Enablement Services server Release 6.1.

Note:

Any HTTP or HTTPS based proxy will not work with the proprietary protocol used in Client Enablement Services. Therefore, you cannot establish a connection among the Avaya one-X® Mobile client application 6.1, the Client Enablement Services and the handset server using such proxies.

Related topics:

[Overview of user data migration from Avaya one-X Mobile 5.2 server](#) on page 223

[Exporting user data from the Avaya one-X Mobile 5.2 server](#) on page 223

Overview of user data migration from Avaya one-X® Mobile 5.2 server

You can use the Avaya one-X® Mobile data migration tool to export user data from the Avaya one-X® Mobile server Release 5.2 to a CSV file. You can use this CSV file to perform a bulk import of users to the Client Enablement Services server.

The CSV file has following information of Avaya one-X® Mobile users:

- User name
- Telephony server
- Telephony extension
- Mobile number
- Voice mail server
- Voice mail mailbox

Avaya one-X® Mobile server Release 5.2 did not support presence functionality. Therefore, the CSV file does not have presence details for users. However, you can manually enter Presence, Conferencing, and Personal contact details in the CSV file.

You can view the logs generated for this utility at the following location: `C:\tmp\migr.log`

Exporting user data from the Avaya one-X® Mobile 5.2 server

Procedure

1. Copy the `MobileMigration.tar` file from the Client Enablement Services server.

   The `MobileMigration.tar` file is at the following location: `/opt/avaya/1xp/`
2. Save this file on any computer from which you can access the Avaya one-X® Mobile server.
3. Create a temporary directory for logging.

   You must create the directory in the C drive.

   For example, `C:\tmp directory`.
4. Extract the `MobileMigration.tar` file.

You can extract this file on any location.

5. From the location where you have extracted the files, copy the `installScript.bat` file and the `oneXMProc.sql` file on the Avaya one-X® Mobile server.

   You must make sure that both files are at the same location.

6. On the Avaya one-X® Mobile Server, execute the `installScript.bat` file.

7. Enter the IP address of the Avaya one-X® Mobile server when the utility prompts for the server IP address.

8. From the location where you have extracted the files, open the `1xm.properties` file and enter following details:

   a. In **1xm_server_ip** property, enter the IP Address of the Avaya one-X® Mobile server.

   b. In **exportFileName** property, enter the file name that you plan to use to export user data from the Avaya one-X® Mobile server.

      Default name of the file is `test.csv`. You can change the name of the file, but the file name must end with a .csv extension. For example, `Exportedusersfile.csv`

9. From the location where you have extracted the files, execute the `startMigration.bat` file.

   This file starts exporting data from the Avaya one-X® Mobile server to the CSV file mentioned in the `1xm.properties` file.

10. Modify the exported CSV file, if required.

    You can modify the handles of servers, or add information about other functionalities that the Avaya one-X® Mobile server does not support such as Personal contact, Presence, Conferencing.

11. Import users to the Client Enablement Services server using this CSV file as an input.

    For more information on the procedure to import users, see Import users on page 198.

    Note:

    The handle of the servers such as Communication Manager, Voice Messaging in the exported CSV file must match with the handle of these servers specified in the Client Enablement Services server. If the handles do not match, then you must manually change the handles in the exported file so that they match. If the handles do not match, the import process fails.

Dial plan migration

Migrating dial plan data from Avaya one-X® Portal 5.2 server to Client Enablement Services 6.1 server

Use the following procedure to migrate dial plan from Avaya one-X® Portal 5.2 server to Client Enablement Services 6.1 server, when the dial plan configuration does not change for the associated back end telephony servers.

The telephony server's definitions configured on Client Enablement Services 6.1 server, the target system for the migration activity, should not contain links to any dial plans.

During the migration, the system removes and recreates the complete dial plan data on the target system. After importing the dial plan rules, you should link the server definitions to the appropriate dial plans.

Related topics:

Exporting dial plan data from the Avaya one-X Portal 5.2 server on page 225

Importing dial plan data to the Avaya one-X Client Enablement Services 6.1 server on page 226

Exporting dial plan data from the Avaya one-X® Portal 5.2 server

Procedure

1. In the SSH terminal session on the Avaya one-X® Portal 5.2 server, log in as root.
2. Copy or download the `export_dialplan.sh` and `export_diaplan.ddl` scripts to the Avaya one-X® Portal 5.2 server, under the `/opt/avaya/1xp` directory.
3. Change to the `/opt/avaya/1xp` directory using the command: `cd /opt/avaya/1xp`
4. Change file permissions to 755 using the command: `chmod 755 export_dialplan.*`
5. Convert the file to UNIX format using the command: `dos2unix export_dialplan.sh`
6. Log in as database instance owner using the command: `su - dbinst`
7. Change to the `/opt/avaya/1xp` directory using the command: `cd /opt/avaya/1xp`

8. Export the dial plan information from Avaya one-X® Portal 5.2 server using the command: `./export_dialplan.sh`
   The script produces following output files in the `/tmp` directory:
   - `dialPlan.del`
   - `dialPlanExpression.del`

   These files contain the exported data.

Importing dial plan data to the Avaya one-X® Client Enablement Services 6.1 server

Before you begin

You must set up the CLI client on the Client Enablement Services 6.1 before proceeding with the dial plan data migration. For procedure, see Prerequisite settings on Linux on page 193.

Procedure

1. Copy the `dialPlan.del` and `dialPlanExpression.del` files on the Client Enablement Services 6.1 server to the `/tmp` directory.
2. In the SSH terminal session on the Client Enablement Services 6.1 server, log in as root.
3. Copy or download the `import_dialplan.sh` and `import_diaplan.ddl` scripts, if not present, to the Client Enablement Services 6.1 server, under the `/opt/avaya/1xp` directory.
4. Change to the `/opt/avaya/1xp` directory using the command: `cd /opt/avaya/1xp`
5. Change file permissions to 755 using the command: `chmod 775 import_dialplan.*`
6. Convert the file to the UNIX format using the command: `dos2unix import_dialplan.sh`
7. Log in as database instance owner using the command: `su - dbinst`
8. Change to the `/opt/avaya/1xp` directory using the command: `cd /opt/avaya/1xp`
9. Import the dial plan data to the Client Enablement Services 6.1 server using the command: `./import_dialplan.sh`
   The system imports the data to the Client Enablement Services database. The script produces the `import_msg.txt` log file for the database import operations in the `/tmp` directory.

> **Note:**
>
> If the dial plan import fails, change the permissions of the files `dialPlanExpression.del` and `dialPlan.del` to 777. Repeat steps 1 to 9.

10. Log in to the Client Enablement Services administration application and assign the dial plans to the existing Telephony, Voice Messaging, and Conference systems.

Example

Sample output for import script execution:

```
Database Connection Information
Database server        = DB2/LINUXX8664 9.7.0
SQL authorization ID   = DBINST
Local database alias   = ACPDB
DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.
Number of rows read         = 3
Number of rows skipped      = 0
Number of rows inserted     = 3
Number of rows updated      = 0
Number of rows rejected     = 0
Number of rows committed    = 3
Number of rows read         = 13
Number of rows skipped      = 0
Number of rows inserted     = 13
Number of rows updated      = 0
Number of rows rejected     = 0
```

Related topics:

Prerequisite settings on Linux on page 193

Migrating dial plan data from the Client Enablement Services 6.1 server to another Client Enablement Services 6.1 server

Use the following procedure to migrate the dial plan from a Client Enablement Services 6.1 server to another Client Enablement Services 6.1 server, when the dial plan configuration does not change for the associated back end telephony servers.

The telephony server's definitions configured on the new Client Enablement Services 6.1 server, the target system for the migration activity, should not contain links to any dial plans.

During the migration, the system removes and recreates the complete dial plan data on the target system. After importing the dial plan rules, the Client Enablement Services administrator should link the server definitions to the appropriate dial plans.

Related topics:

Prerequisite settings on Linux on page 193

Exporting dial plan data from the Client Enablement Services 6.1 server on page 228

Importing dial plan data to the Avaya one-X Client Enablement Services 6.1 server on page 229

Exporting dial plan data from the Client Enablement Services 6.1 server

Before you begin

You must set up the CLI client on the Client Enablement Services 6.1 before proceeding with the dial plan data migration. For procedure, see Prerequisite settings on Linux on page 193.

Procedure

1. In the SSH terminal session on the Client Enablement Services 6.1 server, log in as root.
2. Change to the `/opt/avaya/1xp` directory using the command: `cd /opt/avaya/1xp`

   The `export_dialplan.sh` and `export_diaplan.ddl` scripts are available in the `/opt/avaya/1xp` directory.
3. Change file permissions to 755 using the command: `chmod 755 export_dialplan.*`
4. Convert the file to UNIX format using the command: `dos2unix export_dialplan.sh`
5. Log in as database instance owner using the command: `su - dbinst`
6. Change to the `/opt/avaya/1xp` directory using the command: `cd /opt/avaya/1xp`
7. Export the dial plan information from Client Enablement Services 6.1 server using the command: `./export_dialplan.sh`
   The script produces following output files in the `/tmp` directory.

   - `dialPlan.del`
   - `dialPlanExpression.del`

   These files contain the exported data.

Importing dial plan data to the Avaya one-X® Client Enablement Services 6.1 server

Procedure

1. Copy the `dialPlan.del` and `dialPlanExpression.del` files on the Client Enablement Services 6.1 server to the `/tmp` directory.
2. In the SSH terminal session on the Client Enablement Services 6.1 server, log in as root.
3. Copy or download the `import_dialplan.sh` and `import_diaplan.ddl` scripts, if not already present, to the Client Enablement Services 6.1 server, under the `/opt/avaya/1xp` directory.
4. Change to the `/opt/avaya/1xp` directory using the command: `cd /opt/avaya/1xp`
5. Change file permissions to 755 using the command: `chmod 775 import_dialplan.*`
6. Convert the file to the UNIX format using the command: `dos2unix import_dialplan.sh`
7. Log in as database instance owner using the command: `su - dbinst`
8. Change to the `/opt/avaya/1xp` directory using the command: `cd /opt/avaya/1xp`
9. Import the dial plan data to the Client Enablement Services 6.1 server using the command: `./import_dialplan.sh`
   The system imports the data to the Client Enablement Services database. The script produces the `import_msg.txt` log file for the database import operations in the `/tmp` directory.

   Note:

   If the dial plan import fails, change the permissions of the files `dialPlanExpression.del` and `dialPlan.del` to 777. Repeat steps 1 to 9.
10. Log in to the Client Enablement Services administration application, and assign the dial plans to the existing Telephony, Voice Messaging, and Conference systems.

Example

Sample output for import script execution:

```
Database Connection Information
Database server        = DB2/LINUXX8664 9.7.0
SQL authorization ID   = DBINST
Local database alias   = ACPDB
```

```
DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.
Number of rows read         = 3
Number of rows skipped      = 0
Number of rows inserted     = 3
Number of rows updated      = 0
Number of rows rejected     = 0
Number of rows committed    = 3
Number of rows read         = 13
Number of rows skipped      = 0
Number of rows inserted     = 13
Number of rows updated      = 0
Number of rows rejected     = 0
```

Chapter 9: Template and database backup and restore

Backup and restore overview

Back up and restore the Client Enablement Services template by using the System Platform backup and restore procedure. Template backup includes a back up of the database, server files, handset server, and audio transcoding server.

You can also schedule regular backups of the Client Enablement Services server database using the Database Backup scheduler feature of the Client Enablement Services administration application. Database backup scheduler creates a backup of the database in the location specified in the **Backup File to Location** field. This file is deleted when you either install or upgrade the Client Enablement Services template.

Some key points of these backup and restore procedures:

- System Platform backup
    - backs up the template, not only the database.
    - stops and starts the WAS, therefore, Client Enablement Services service is not available at the time of backup and restore
    - allows remote backup.
- Client Enablement Services scheduler backup
    - backs up only the database.
    - interrupts only the database operations.
    - does not allow remote backup.
- System Platform restore
    - stops and starts WAS automatically.
- Client Enablement Services restore
    - administrator has to manually stop the WAS first and then follow the steps to restore the backup.

Backing up System Platform

System Platform backup

You can back up configuration information for System Platform and the solution template (all template virtual machines).

Note:

The *solution template* is the Client Enablement Services server template.

System Platform backs up sets of data and combines them into a larger backup archive. Backup sets are related data items available for backup. When you perform a back up, the system executes the operation for all backup sets. All backup sets must succeed to produce a backup archive. If any of the backup set fails, then the system removes the backup archive. The amount of data backed up depends on the specific solution template.

The system stores the backup data in the `/vspdata/backup` directory in Console Domain. This is a default location. During an upgrade, the system does not upgrade the `/vspdata` folder, facilitating a data restore operation if required. You can change this location and back up the System Platform backup archives to a different directory in System Platform or in an external server. Optionally, send the backup data to an external e-mail address if the file size is smaller than 10 MB.

If a backup fails, the system automatically redirects to the Backup page after login and displays the following message: `Last Backup Failed`. The system continues to display the message until a backup succeeds.

Note:

The System Platform backup feature does not back up the following types of configuration data:

- System parameters (examples: SNMP Discovery, Template product ID)
- Networking parameters (examples: Template IP and hostname, Console Domain IP and hostname, static IP route configuration)
- Ethernet parameters (examples: Auto-negotiation, speed and port information)
- Security configuration (examples: SSH keys, Enable Advance password, Host access list)

  In scenarios where, for example, an administrator performs a system backup prior to a template or platform upgrade or platform replacement, and the system generates new unique SSH keys internally as part of the upgrade or replacement action. The SSH keys generated prior to the backup operation are of no use to the system updated or replaced.

Note:

You cannot restore an older version of System Platform from a backup set created on a newer version of System Platform.

Backing up the system

About this task

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 232.

Note:

The *solution template* is the Client Enablement Services server template.

Note:

During the backup process, the Client Enablement Services service is interrupted for five to ten minutes. The interruption time depends on the size of the database server that you are backing up.

Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

Note:

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Related topics:

Backup field descriptions on page 236

Scheduling a backup

About this task

Use this procedure to back up System Platform and the solution template on a regular basis. Backups are not scheduled by default on System Platform.

Note:

During the backup process, the Client Enablement Services service is interrupted for five to ten minutes. The interruption time depends on the size of the database server that you are backing up.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select **Schedule Backup**.
4. Specify the following:
    - **Frequency**
    - **Start Time**
    - **Archives kept on server**.
    - **Backup Method**

      Use this field to copy the backup archive file to a remote server or to send the file to an e-mail address. The file is also stored on the on the System Platform server.
5. Click **Schedule Backup**.

Related topics:

Backup field descriptions on page 236

Transferring the Backup Archives to a remote destination

About this task

You can send the backup archive to a mail address or to a remote server by SFTP with using the **Backup Method** option.

Procedure

1. To send the archive by email:
    a. Select the **Email** option as the **Backup Method**.
    b. Specify the **Email Address** and the **Mail Server**.
2. To send the archive to a remote server by SFTP:
    a. Select **SFTP** option as the **Backup Method**.
    b. Specify the **SFTP Hostname** (or IP Address), Directory to which the archive will be sent and the username and password to log in the server.

Viewing backup history

About this task

Use this procedure to view the last 10 backups executed and their status. If the last backup failed, the system automatically redirects you to the Backup page after login and displays the following message: `Last Backup Failed`. The system continues to display the message until a backup is successful.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select **Backup History**.

    The system displays the last 10 backups executed with their dates and the status.

Backup field descriptions

Use the Backup page to back up configuration information for System Platform and the solution template.

Backup Now fields

The following table describes the fields that are displayed if you select **Backup Now** at the top of the Backup page.

Field Names	Descriptions
Backup Method	Select a location to send the backup file: • **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory. • **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server. Enter the hostname, directory, user name, and password for the SFTP server. • **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server. Enter the e-mail address and the server address of the recipient.
Backup Now	Starts the backup operation.

Schedule Backup fields

The following table describes the fields that are displayed if you select **Schedule Backup** at the top of the Backup page.

Field Names	Descriptions
Frequency	Select one of the following options: • Daily • Weekly • Monthly
Start Time	The start time for the backup.
Archives kept on the server	The number of backup archives to store on the System Platform server. The default is 10.

Field Names	Descriptions
Backup Method	Select a location to send the backup file: • **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory. • **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server. Enter the hostname, directory, user name, and password for the SFTP server. • **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server. Enter the e-mail address and the server address of the recipient.
Schedule Backup	Schedules the backup process.
Cancel Schedule	Cancels an existing backup schedule.

Related topics:

Backing up the system on page 233
Scheduling a backup on page 234

Restoring System Platform

Restoring backed up configuration information

About this task

To restore backed up configuration information for System Platform and the Solution Template (all virtual machines), use this procedure.

Note:

Do not attempt to use restore functionality to make networking changes. Perform networking changes only from the Network Configuration page of the Web Console.

Note:

You cannot restore an older version of System Platform from a backup set created on a newer version of System Platform.

Note:

The *solution template* is the Client Enablement Services server template.

Note:

During the restore process, the Client Enablement Services service is interrupted for 20 – 45 minutes. The restore time depends on the size of the database that you are using for the restore.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Restore**.
   The Restore page displays a list of previously backed up archives on the System Platform system.
3. Select an archive file from the list, and then click **Restore** to restore from the selected archive.

   To restore an archive, restart the System Platform Web Console. Log in again after the restore operation is complete.

Related topics:

System Platform backup on page 232
Restore field descriptions on page 238

Restore field descriptions

Field Names	Descriptions
Restore from	Select the location of the backup archive file from which you must restore configuration information. • **Local**: Restores from a file on System Platform. If you select this option, the Restore page displays a list of previously backed up archives on the System Platform system. • **SFTP**: Restores from a file on a remote server. If you select this option, enter the hostname or IP address of the remote server, directory where the archive file is

Field Names	Descriptions
	located, and user name and password for the SFTP server. • **Upload**: Restores from a file on your computer.
Archive Filename	Filenames of the backup archive files at the location you specify.
Archive Date	Date that the file was created.
Selection	Select this check box to restore from the archive file.
Restore History	Displays the restore history for the last ten restores. If an error occurred during the last restore, the system directs you to this page after login and continues to display an error message until a restore is successful.

Button descriptions

Button	Description
Search	Displayed if you select **SFTP**. Searches for archive files in the specified directory of the remote server.
Clear Search Result	Clears the list of archive files found on a remote server after an SFTP search.

Related topics:

Restoring backed up configuration information on page 237

Viewing restore history

About this task

Use this procedure to view the last 10 restores executed and their status. If the last restore failed, the system automatically redirects you to the Restore page after login and displays the following message: `Last Restore Failed`. The system continues to display the message until a restore is successful

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Restore**.

3. On the Restore page, select the **Restore History** option.

Backing up and restoring the database

You can schedule regular backups of Avaya one-X® Client Enablement Services database. Use this database backup file to restore the database in case of any problem with the database.

Related topics:

Scheduling Database Backup on page 129

Backing up the database

Before you begin

Before you follow these steps, log out of the Client Enablement Services administration application and log back in to make sure there are no active administration sessions running while you take a back up of the database.

About this task

You should do a database backup during off hours because it takes the database off line.

Procedure

1. Save the Client Enablement Services system configuration file such as `1XPAdvancedRegistry.properties.locked`.

   The location of this file is:

   - `/opt/IBM/WebSphere/AppServer/profiles/default/properties/1XPAdvancedRegistry.properties.locked`

   Note:

   Client Enablement Services creates the `1XPAdvancedRegistry.properties.locked` file only if the custom registry is being used and when the Split Domain topography is implemented within Active Directory.

2. Perform database backups regularly using the procedures provided in Scheduling Database Backup on page 129.
   The scheduler database backup creates a file with the name of the database and the time of the backup.

3. Save this file.

Use this file when you restore the database.

Example

Back up the following files to a remote system:

- Keystores
  - From the `/opt/IBM/HTTPServer/` folder: `ihsserverkey.kdb`, `ihsserverkey.rdb`, and `ihsserverkey.sth`.
  - In a co-resident handset server, from the `/opt/avaya/HandsetServer/` folder: `keystore.jks`
- Other files
  - /etc/hosts
  - /etc/resolv.conf
  - /opt/avaya/HandsetServer/handset_server.properties
  - $WAS_HOME/lib/ext/HandsetServices.properties

Restoring the Client Enablement Services database

Before you begin

Do not restore the database while the Client Enablement Services system is running.

About this task

Use these steps when you restore the database either after a system failure or when you upgrade your system. You must use the same file created during the database backup for the restore process.

Procedure

1. Stop the Client Enablement Services server by logging as root to the Client Enablement Services server. Use the command **`service 1xp stop`** to stop the server.

   For more information, see Stopping Client Enablement Services on page 300.

2. Type **`su — dbinst`** to log in to the *dbinst* account that is created when you install the Client Enablement Services system.

   dbinst is the default name for the account. If you have renamed this account after the installation, log in to the renamed account.

3. Copy your system configuration files, such as `1XPAdvancedRegistry.properties.locked` to the directory where the database resides on the Client Enablement Services server.

4. Copy the backup database file to the directory where the existing backups reside on the Client Enablement Services server.
5. From the command line prompt, go to `/opt/avaya/1xp`.
6. Type **`./db2RestoreToExisting.sh`** to display the usage requirements of the shell script.

   Usage:`./db2RestoreToExisting.sh ACPDB <from directory> <from time>`. For example, suppose a database has the following directory locations:

   `<from directory>: /opt/avaya/1xp/dbbackup`

   `<from time>: 20080801102735`

   The syntax for this appears as shown below:

   ```
   ./db2RestoreToExisting.sh ACPDB /opt/avaya/1xp/dbbackup/
   20080801102735
   ```

   Note:

   You can derive the time (20080801102735) from the file name of the backup file that you are using for the restore.

   The backups are normally written to the `<from directory>` path.

7. Type `db2stop` and press Enter.
8. Type `db2start` and press Enter.
9. Type `exit` to exit from user dbinst.
10. Run the following command to restart the IBM WebSphere server: **`service 1xp start`**
11. Import the Modular Messaging certificates. This trust store certificate is lost in the manual backup and restore process.

    For detailed steps see Installing the voice messaging server security certificates on page 54.

Example

Restore the following files:

- Keystores
  - To the `/opt/IBM/HTTPServer/` folder: `ihsserverkey.kdb`, `ihsserverkey.rdb`, and `ihsserverkey.sth`.

    Ensure that for all ihs keystore files the ownership is set to root.root and permissions set asrw-r--r--
  - To the`/opt/avaya/HandsetServer/` and `$WAS_HOME/lib/ext/` folders: `keystore.jks`.

Ensure that the ownership is set to root.appsvr and permissions set as rw-r-----

- Other files
  - `/etc/hosts`
  - `/etc/resolv.conf`
  - `/opt/avaya/HandsetServer/handset_server.properties`

    Ensure that the ownership is set to appsvr.appsvr and permissions set as rw-r--r--
  - `$WAS_HOME/lib/ext/HandsetServices.properties`

    Ensure that the ownership is set to appsvr.appsvr and permissions set as rw-r--r--

Managing disk space on the Avaya one-X® Client Enablement Services template

About this task

In Client Enablement Services release 6.1, the disk space is 30 GB, therefore, you must periodically monitor the disk space on the server and make sure enough space is available for the files created through logging and database backups. The database backup file size is dependent on the installation. You must periodically move the database backup files to an external location after the database backup is complete. Database backups are scheduled periodically through the Client Enablement Services administration application. You can also adjust the frequency of the backup scheduled through the administration application along with periodically checking the availability of free space.

If there is not enough space for a database backup, the backup fails and the system displays the following error message:

```
Not enough disk space.
```

The system also raises an alarm when the database backup fails. You can check the details in the `trace.log` file. In case of a database failure, you must free the space by copying the files to a remote storage location.

To avoid database backup failure, Avaya recommends that you have free space that equals a total of all the following measures:

- Space equal to or more than three times the database backup file size.
- Space for system swap that is approximately 2 GB.
- Space that the generated logs occupy.

Perform the following steps for monitoring the disk space:

Procedure

1. Log in to the Client Enablement Services CLI as a craft user and the switch to the root user.

2. To view the free disk space, run the command: **`df`**
   The value in **Use %** column displays the disk space already filled. The occupied disk space must not exceed 75% of the available disk space. If the **Use%** column value is approaching 75%, follow step 3.
3. Copy the files that are needed from the `/opt/avaya/dbbackup/` folder to an external location.
4. Delete the files that are not required in the `/opt/avaya/dbbackup/` folder to free the disk space.

Next steps

You can monitor the log file of the Handset Server at the location `/opt/avaya/HandsetServer/logs/server.log`. The startup script redirects stdout to this file. You can periodically clean this file by using the command: **`rm /opt/avaya/HandsetServer/logs/server.log`**

Other log files such as trace logs, error logs, system logs, and service logs are rolled over. You can configure the size of these files from the administration application.

Related topics:

Scheduling Database Backup on page 129
Logging on page 159

Chapter 10: Configuring other products for Avaya one-X® Client Enablement Services

Installing required components for integrated servers

Before you begin

If a supported version of the integrated server software is already functional in the enterprise and the system meets the version and user requirements, you do not need to install a new system. You can integrate Avaya one-X® Client Enablement Services with the existing system.

About this task

You must perform administration of following components before configuring the Client Enablement Services administration application.

- Communication Manager
- Modular Messaging or Avaya Aura® Messaging or Communication Manager Messaging
- Conferencing
- Presence Services
- Session Manager
- System Manager

The names of the following installation and administration documents were current when *Administering Avaya one-X® Client Enablement Services* was published. Review the documentation set provided with your software to ensure that you use the correct document to install and configure the components.

Note:

This chapter lists only those steps that are required for integration of the other Avaya product with Client Enablement Services.

Procedure

1. Install and configure all required components for servers you want to integrate with Client Enablement Services.

Component	Documentation
Communication Manager	• *Installing and Configuring Avaya Aura® Communication Manager* • *Administering Avaya Aura® Communication Manager*
Modular Messaging	• *Modular Messaging for the Avaya Message Storage Server (MSS) Configuration Installation and Upgrades* • *Installing Avaya Modular Messaging on a Single Server Configuration* • *Modular Messaging Admin Guide with Avaya MSS*
Avaya Aura® Messaging	• *Administering Avaya Aura® Messaging*
Communication Manager Messaging	• *Avaya Aura® Communication Manager Messaging Documentation Library*
Conferencing	• *Implementing Avaya Aura® Conferencing* • *Operating Avaya Aura® Conferencing*
Presence Services	• *Installing Avaya Aura® Presence Services* • *Administering Avaya Aura® Presence Services*
Session Manager	• *Implementing Avaya Aura® Session Manager* • *Administering Avaya Aura® Session Manager*
System Manager	• *Installing and Upgrading Avaya Aura® System Manager* • *Administering Avaya Aura® System Manager*

2. Follow the documentation provided with the required Avaya components, and install the required licenses.

Interoperability matrix of supported Avaya products

Avaya components	Software	Supported versions	Maximum number of configuration supported
PBX	Avaya Aura® Communication Manager	5.2.1 SP11, 6.0, 6.0.1 SP6, 6.2 SP3 Communication Manager 6.0 is supported only as an evolution server.	4
Session Manager	Avaya Aura® Session Manager	6.0, 6.1SP7, 6.2 SP1	4
System Manager	Avaya Aura® System Manager	6.1SP7 and 6.2 SP1	1
Presence	Avaya Aura® Presence Services	6.1 SP3	1
Messaging	Avaya Modular Messaging	5.2 SP6	4
	Avaya Aura® Messaging	6.0, 6.0.1, 6.1 SP1, 6.2	
	Communication Manager Messaging	6.2	
Conferencing	Avaya Aura® Conferencing Standard Edition In Release 5.2.1, Avaya Aura® Conferencing Standard Edition was Avaya Meeting Exchange™ Enterprise Edition.	5.2.1, 6.0	3
Avaya one-X® Portal	Avaya one-X® Portal	5.2 SP4 There are limitations in the interoperability between the Avaya one-X® Portal client application and the Client Enablement Services client	

Avaya components	Software	Supported versions	Maximum number of configuration supported
		applications. For more information on this, see the Client Enablement Services and Avaya one-X® Portal interoperability section in the Client Enablement Services release notes document for Release 6.1 SP3.	

Minimum components required for Avaya one-X® Client Enablement Services features

Feature	Minimum components required for integration with Client Enablement Services
Telephony (H.323)	Communication Manager
Telephony (SIP and H.323)	Communication Manager, Session Manager, and System Manager
Presence*	Communication Manager, Session Manager, System Manager, and Presence Services
Messaging	Communication Manager and Modular Messaging Or Communication Manager, Session Manager, System Manager, and Avaya Aura® Messaging Or Communication Manager and Communication Manager Messaging
Conferencing	Communication Manager and Avaya Meeting Exchange™ Enterprise Edition. Or Communication Manager, Session Manager, System Manager, and Avaya Aura® Conferencing Standard Edition

* For retrieving the presence of H.323 telephone extensions, you do not need to integrate Application Enablement Services with Client Enablement Services, but you must integrate Application Enablement Services with Presence Services and Communication Manager.

Configuring Communication Manager for Avaya one-X® Client Enablement Services

Enabling one-X Server Access on Communication Manager

About this task

On Communication Manager, you must ensure that the **one-X Server Access** field is enabled in the COR assigned to the extension of the user.

Procedure

1. On Communication Manager, open the COR using the command : `change COR<`*`COR number assigned to the user extension`*`>`
2. On page 3 of the COR, ensure that the **one-X Server Access** field is set to **Y**.

   By default this field is set to **Y**.

   If this field is set to **N**, Client Enablement Services features such as call handling and call logging do not work on the client applications.
3. Set the value of **IP Softphone** for the telephone extension of each Client Enablement Services user.
   a. Use the `change station` command to navigate to the Station screen.
   b. Set the value of **IP Softphone** to `y`.
   c. If it is a SIP extension, then go to page 6 and change the **Type of 3PCC Enabled** field to **None**.
   d. Press `Enter` to save.

Configuring the Feature-Related System Parameter screen

About this task

When a user enables the desk phone ringer OFF option in the Avaya one-X® Mobile client application, the desk phone ringer is turned off, but the desk phone must log the caller name and number in the call logs history.

This feature is available only on desk phones with H.323 extensions.

Procedure

1. Log in to Communication Manager.
2. Type the command **`display system-parameters features`**
3. On the FEATURE-RELATED SYSTEM PARAMETERS screen, set the **Keep Bridged Information on Multiline Displays During Calls?** field to **y**.
   The desk phone logs all calls when the desk phone ringer OFF option is enabled on the Avaya one-X® Mobile client application.
4. On the FEATURE-RELATED SYSTEM PARAMETERS screen, set the **Automatic Exclusion by COS** field to **n**.

   Callback functionality does not work in the Avaya one-X® Mobile client application if the **Automatic Exclusion by COS** field is set to **y** for the user station on Communication Manager.

Related topics:

Assigning a Mobile Telephony resource to a user on page 113

Adding IP address of Client Enablement Services server

About this task

To establish communication between Client Enablement Services and Communication Manager, add the IP address of the Client Enablement Services server in the node-name list of Communication Manager.

Procedure

1. Log in to Communication Manager.
2. At the command prompt, type **change** *`node-names ip`*.
3. In the **Name** field, enter the machine name of the Client Enablement Services server.
4. In the **IP Address** field, enter the IP address of the Client Enablement Services server.

Next steps

Adding a signaling group.

Adding a signaling group

About this task

To establish communication between Client Enablement Services and Communication Manager, use a SIP signaling group.

Client Enablement Services can connect to Communication Manager through Session Manager only when you create a SIP signaling group and trunk group is set between Communication Manager and Session Manager.

Procedure

1. Log in to Communication Manager.
2. At the command prompt, type `add signaling group<`*`group number`*`>`.
3. In the **Transport Method** field, type `TCP` for non-secure communication and `TLS` for secure communication.

   Note:

   The **Far-end Listen Port** and **Near-end Listen Port** numbers automatically change to the default values for the **Transport Method** selected. Therefore, you must check the port numbers after setting a **Transport Method** to make sure you are setting the correct port numbers.
4. In the **Far-end Node Name** field, enter the name of the far-end node.
5. In the **Near-end Node Name** field, enter the name of the near-end node.
6. In the **Far-end Listen Port** field, enter the number of the far-end listen port.
7. In the **Near-end Listen Port** field, enter the number of the near-end listen port.
8. In the **Near-end Network Region** field, enter the number of the near-end network region.
9. In the **Far-end Domain** field, enter the domain.

   The domain should be same as the domain for SIP Local server defined in the Client Enablement Services administration application.

   Note:

   If you have specified the **Far-end Domain** field in the signaling channel, make sure you set the same value in the **Domain** field of the SIP Local Configuration page in Client Enablement Services administration application and in the **Far-end Domain** field of the signaling channel on Communication Manager.

Next steps

Adding a SIP trunk group.

Checking the status of a signaling group

About this task

To check whether the signaling group is running successfully, perform the following steps:

Procedure

At the Command Prompt, type **`status signaling-group`** *`<signaling group number>`*.

The system displays the status of the signaling group.

Example

If the system displays *Group State: in-service*, it indicates that the signaling group is running successfully.

Adding a SIP trunk group

About this task

To establish communication between Client Enablement Services and Communication Manager, use a SIP trunk group.

Client Enablement Services can connect to Communication Manager through Session Manager only when you create a SIP signaling group and trunk group is set between Communication Manager and Session Manager.

Procedure

1. Log in to Communication Manager.
2. At the Command Prompt, type **`add trunk-group`** *`<trunk group number>`*.
3. In the **Group Type** field, type `SIP`.
4. In the **Group Name** field, enter the name of the SIP trunk group.
5. In the **TAC** field, enter the name of the trunk access code.
6. In the **Outgoing Display** field, type Y.
7. In the **Service Type** field, type the service type as `tie`.
8. In the **Signaling Group** field, enter the number of the signaling group.

Next steps

Checking status of SIP trunk group

Checking the status of a SIP trunk group

Procedure

At the command prompt, type **`status trunk`** *`<trunk group number>`*.
The system displays the status of the SIP trunk.

- If the trunk is active, the status is `in-service/idle` and the connected ports busy status is `no`.
- If the trunk is down, the status is `Out-of-service-NE` and the connected ports busy status is `no`.

Enabling secure SIP communication between Avaya one-X® Client Enablement Services and Communication Manager 5.2.1 using CLI

Procedure

1. On the Client Enablement Services administration application,
   a. Click the **Monitors** tab.
   b. Click **Telephony**.
   c. On the Monitor Telephony Services page, if the **State** of **SipService** is **Connected**, click **Suspend** to stop the service.
2. Log on to the IBM Web console: `https://`*`<IP address or FQDN _OF_CES>`*`:9043/ibm/console`, and perform the following steps:

   The log-on credentials is same as the Client Enablement Services service account.

   a. Go to **SSL certificate and key management** > **Key stores and certificates** > **NodeDefaultTrustStore** > **Signer certificates**.
   b. From the list of certificates, select the certificate with the value **O=AVAYA, OU=MGMT, CN=default** in the **Issued to** column.
   c. Click **Extract**.
   d. In the **Save** dialog box, enter a name for the certificate and keep the default data type .
   e. Click **OK**.
   This saves the certificate, and the message displayed tells you the location where the certificate is stored.
   f. Copy this certificate in Communication Manager in the `/var/home/ftp/pub` directory.

3. Perform the following steps in Communication Manager to install the certificate on Communication Manager:
    a. Putty in as a super user.
    b. Go into the bash shell and issue the command `tlscertmanage -i filename`.
    c. To verify that the certificate got installed, issue the command `tlscertmanage -l`.
    d. Restart the Communication Manager.
    e. Change the transport method to TLS in the Signaling group of Communication Manager. See Adding a signaling group on page 251.
    f. In the Communication Manager CLI, use the **`save translation`** command to save the translations on the Communication Manager.
4. In the Client Enablement Services administration application, go to **System** > **SIP Local**.
    a. Select the **Secure Port** check box.
    b. Change the **Port** to the port used by Client Enablement Services for secure connection.
    c. Click **Save**.
5. Go to **Servers** >**Telephony**.
    a. On the Telephony Servers page, click the handle of the Communication Manager you want to modify.
    b. On the View Telephony Server page, change the **SIP Remote Port** to the port number configured on the Communication Manager.
    c. Select the **SIP Remote Secure** check box.
    d. Click **Save**.
6. Go to **Monitors** > **Telephony**.
7. On the Monitor Telephony Services page, in the **SipService** section, click **Resume** to start the service.

Enabling secure SIP communication between Avaya one-X® Client Enablement Services and Communication Manager 6.0 using Web

Before you begin

If the Client Enablement Services server is not integrated with System Manager, the certificate required for secure connection is not available in WebSphere.

Therefore, for configuring a TLS connection between the Client Enablement Services server and Communication Manager, the Client Enablement Services server must be integrated with System Manager during installation.

Procedure

1. On the Client Enablement Services administration application,
   a. Click the **Monitors** tab.
   b. Click **Telephony**.
   c. On the Monitor Telephony Services page, if the **State** of **SipService** is **Connected**, click **Suspend** to stop the service.
2. Log on to the IBM Web console: `https://`*`<IP address or FQDN _OF_CES>`*`:9043/ibm/console`, and perform the following steps:

   The log-on credentials is same as the Client Enablement Services service account.

   a. Go to **SSL certificate and key management** > **Key stores and certificates** > **NodeDefaultTrustStore** > **Signer certificates**.
   b. From the list of certificates, select the certificate with the value **O=AVAYA, OU=MGMT, CN=default** in the **Issued to** column.
   c. Click **Extract**.
   d. In the **Save** dialog box, enter a name for the certificate and keep the default data type.
   e. Click **OK**.
   This saves the certificate, and the message displayed tells you the location where the certificate is stored. The certificate should be with .pem extension.
   f. Copy this certificate in Communication Manager in the `/var/home/ftp/pub` directory.
3. Perform the following steps in Communication Manager to install the certificate on Communication Manager:
   a. Log in to the Communication Manager System Management Interface (SMI).
   b. Click **Administration** > **Server (Maintenance)**.
   c. Under **Security**, click **Trusted Certificates**.
   d. On the Trusted Certificates page, click **Add**.
   e. On the Trusted Certificate-Add page, enter the file name for the certificate you want to add.

   The certificate must be in a .pem file and in the `/var/home/ftp/pub` directory.

   f. To validate the certificate, click **Open**.

   After a successful validation, the Trusted Certificates-Add page displays the issued-to, issued by, and expiration date information for the certificate you are adding.

   > **Note:**
   >
   > The system displays an error message if the certificate is not a valid certificate.

   g. Enter a name for the certificate.

You must enter the same name for the certificate in each repository.

h. Select the repositories to which you want to add the certificate, and click **Add**.

   Select the Authentication, Authorization and Accounting Services (A) and Communication Manager (C) repositories.

   The system converts the <*certificate_name*>.pem file to a <*certificate_name*>.crt file and verifies the following:

   - The certificate name is unique.
   - The certificate is not a duplicate certificate with a new name.

i. Change the transport method to TLS in the Signaling group of Communication Manager. See Adding a signaling group on page 251.

j. In the Communication Manager CLI, use the **`save translation`** command to save the translations on the Communication Manager.

k. Restart the Communication Manager.

4. In the Client Enablement Services administration application, go to **System** > **SIP Local**.

   a. Select the **Secure Port** check box.
   b. Change the **Port** to the port used by Client Enablement Services for secure connection.
   c. Click **Save**.

5. Go to **Servers** >**Telephony**.

   a. On the Telephony Servers page, click the handle of the Communication Manager you want to modify.
   b. On the View Telephony Server page, change the **SIP Remote Port** to the port number configured on the Communication Manager.
   c. Select the **SIP Remote Secure** check box.
   d. Click **Save**.

6. Go to **Monitors** > **Telephony**.

7. On the Monitor Telephony Services page, in the **SipService** section, click **Resume** to start the service.

Configuring the coverage path in Communication Manager for the Block all calls feature in Avaya one-X® Client Enablement Services

About this task

The Block all calls functionality in Client Enablement Services is similar to the Send All Calls feature in Communication Manager.

Block all calls uses the station coverage path to determine the destination of a call when the user does one of the following:

- Enables the Avaya one-X® Mobile Block all calls feature.
- Clicks **Ignore** when a call arrives in the Avaya one-X® Mobile client application.

⊕ **Tip:**

For more details about these configurations, see *Administering Avaya Aura® Communication Manager*.

Procedure

1. Log in to the Communication Manager using SSH.
2. To change the coverage path for an existing extension, use the `change station <station number>` command.
3. On the STATION page, in the **Coverage Path 1** field, give the number of the required coverage path.

Configuring call forwarding

About this task

Users need additional permissions to forward an external call to a telephone that is not controlled by Communication Manager.

This configuration on Communication Manager causes following problems:

- When you switch off the trunk-to-trunk restriction, a user can use the company trunk to make international calls on behalf of someone else. For example, a user who gets a call from a friend on the business phone number can transfer the call to a common friend overseas on behalf of the first caller.
- In some countries, there is no explicit signaling to indicate to the PBX that the far end has disconnected the call. For example, if a user in the PBX transfers a trunk call to another trunk, both sides are on trunk calls. In this scenario, the PBX cannot detect when to disconnect the call and free up the trunks.

⊕ **Tip:**

For more details about these configurations, see *Administering Avaya Aura™ Communication Manager*.

Procedure

1. Log in to the Avaya Site Administration (ASA) application.
2. In the Class of Service screen:

a. Set the **Trk-to-Trk Restriction Override** to y to enable the trunk-to-trunk transfer permissions for each user.

b. Set the value of **Restrict Call Fwd-Off Net** to n.

3. Press `Enter`.

Extension to Cellular and Client Enablement Services

Do not manually configure the EC500 feature on Communication Manager for the following users:

- Users using the Avaya one-X® Mobile client application in integration with Client Enablement Services Release 6.1. For these users, the Client Enablement Services server sets the telephony settings on the STATION TO OFF-PBX TELEPHONE MAPPING screen to **ONE-X** on Communication Manager when the user goes through the Mobile Setup Wizard after logging in the Avaya one-X® Mobile client application for the first time.
- Users using the UC mode of the Avaya one-X® Mobile client application Release 6.1.2. For these users, the Client Enablement Services server sets the telephony settings on the STATION TO OFF-PBX TELEPHONE MAPPING screen to **ONE-X** on Communication Manager when the user goes through the Mobile Setup Wizard after logging in the Avaya one-X® Mobile client application in the UC mode for the first time.

Related topics:

Assigning a Mobile Telephony resource to a user on page 113

Configuring Avaya Modular Messaging for Avaya one-X® Client Enablement Services

Configuring Modular Messaging ports and protocols

About this task

If you change the default ports for one or more of these protocols in Modular Messaging, you must change the default settings in the Avaya one-X® Client Enablement Services Administration application.

Note:

Client Enablement Services integrates with messaging servers using only the Avaya message store, and not any other e-mail message stores.

Procedure

1. Navigate to the following Modular Messaging administration screen: **Messaging Administration** > **System Administration**.
2. On the System Administration screen, access the fields required to configure and enable the following protocols:
   - IMAP4/SSL
   - SMTP
   - LDAP
3. Validate the port numbers configured for these protocols against the port requirements for Client Enablement Services.

Configuring Modular Messaging LDAP access

Procedure

1. Navigate to the following Modular Messaging administration screen: **Messaging Administration** > **Networked Machine Management**.
2. On the Networked Machine Management screen, set the value of **Updates In** to `Yes` for the Message Storage Server in the Modular Messaging domain.
3. Save the change.
4. Navigate to the **Diagnostic** menu and test the LDAP connection.

Verifying Modular Messaging subscriber values

About this task

For every Avaya one-X® Client Enablement Services user, at least one Modular Messaging subscriber value must match the corresponding value in the Corporate Directory record for the user. If none of these values match, Client Enablement Services cannot accurately link incoming and outgoing communications with the correct users.

Procedure

1. Navigate to the following Modular Messaging administration screen: **Global Administration** > **Subscriber Management**.
2. For all local subscribers, verify that at least one of the following values matches the corresponding value in the user record in Corporate Directory:

- **Telephone Number**
- **PBX extension**
- **Email Handle**
- **Mailbox Number**

Enabling client access for Modular Messaging

About this task

Avaya one-X® Client Enablement Services requires access to the client mailbox. This configuration ensures that subscribers can connect to their mailboxes through Client Enablement Services and access their messages.

Procedure

1. On the MSS, perform the following steps for every Class of Service that is assigned to a subscriber who needs to access messages through Client Enablement Services:
   a. Navigate to the Manage Classes-of-Service page.
   b. In the **Restrict Client Access** field, set the value to No.
   c. Save your changes.
2. On the MAS, in the Voice Mail System Configuration (VMSC) tool:
   a. Navigate to the Messaging selection and view the **General** tab.
   b. Verify that the value of the **Privacy Enforcement Level** is set to one of the following values:
      - Partial
      - Notification Only

      If the Privacy Enforcement Level is set to Full, validate with the customer that you can change the value.
   c. Save your changes.

Establishing trusted connection between the Modular Messaging server and the Client Enablement Services server

About this task

You should add Client Enablement Services in the trusted server list on the Modular Messaging server for allowing it to connect using IMAP and LDAP protocols. Add a trusted link for each of the protocol as per the environment setup.

You must establish a trusted connection on the Modular Messaging server for each Client Enablement Services server in the system.

Procedure

1. Go to **Messaging Administration** > **Trusted Servers**.
2. Click **Add a new trusted server**.
3. Enter the IP address of the Client Enablement Services server and a **Trusted Server Name** and **Password** for this link.

   ✱ **Note:**

   You should use the same login ID and password you used when adding a Voice Messaging server on Client Enablement Services. For more information, see Adding Voice Messaging servers on page 55.
4. If you are using an IMAP connection,
   a. set **IMAP4 Super User Access Allowed** field to **yes**.
   b. if you are using SSL, set **IMAP4 Super User Connection Security** field to **Must use SSL or encrypted SASL**.
5. If you are using an LDAP connection,
   a. set **LDAP Access Allowed** field to **yes**.
   b. depending on the LDAP connection you are using, set **LDAP Connection Security** field to **Must use SSL or encrypted SASL**, if you are using SSL port 636, or set to **No Encryption required** if you are using port 389.
6. Click **Save**.

Configuring Avaya Aura Messaging for Avaya one-X® Client Enablement Services

Configuring Messaging ports and protocols

About this task

If you change the default ports for one or more of these protocols in Messaging, you must change the default settings in the Avaya one-X® Client Enablement Services Administration application.

Note:

Client Enablement Services integrates with messaging servers using only the Avaya message store, and not any other e-mail message stores.

Procedure

1. On the Messaging administration screen, go to **Messaging System** > **System Ports and Access**.
2. In the **System TCP/IP Ports** section, enable the following protocols:
   - **IMAP4 Port**
   - **SMTP Port**
   - **LDAP Port**
3. Validate the port numbers configured for these protocols against the port requirements for Client Enablement Services.

Configuring Messaging LDAP access

Procedure

1. In the Messaging administration screen, go to **Server Settings (Storage)** > **Networked Servers**.
2. On the Manage Networked Servers page, select the local messaging server and click **Edit the Selected Networked Server**.

3. On the Edit Networked Machine page, set the value of **Updates In** to `Yes` for the MSS in the Messaging domain.
4. Click **Save**.
5. Go to **Diagnostics** > **LDAP Test Connection**.

Verifying Messaging subscriber values

About this task

For every Avaya one-X® Client Enablement Services user, at least one Messaging subscriber value must match the corresponding value in the Corporate Directory record for the user. If none of these values match, Client Enablement Services cannot accurately link incoming and outgoing communications with the correct users.

Procedure

1. In the Messaging administration screen, go to **Reports (Storage)** > **Users**.
2. On the Reports page, click the **Mailbox** number of a user.
3. On the User Management > Properties for <user name> page, verify that at least one of the following values match the corresponding value in the user record in Corporate Directory.
    - **Extension**
    - **Internal identifier**
    - **Mailbox number**

    You must verify these values for all local subscribers.

Establishing trusted connection between the Messaging server and the Client Enablement Services server

About this task

You should add Client Enablement Services in the trusted server list on the Messaging server so that they can connect using IMAP and LDAP protocols. Add a trusted link for each protocol as per the environment setup.

You must establish a trusted connection on the Messaging server for each Client Enablement Services server in the system.

Procedure

1. Go to **Messaging** > **Administration** > **Server Settings (Storage)** > **Trusted Servers**.
2. On the Manage Trusted Servers page, click **Add a new trusted server**.
3. On the Add Trusted Server page, enter the IP address of the Client Enablement Services server in the **Machine Name / IP Address** field, a **Trusted Server Name**, and a **Password**.

   ✱ **Note:**

   You should use the same login ID and password you used when adding a Voice Messaging Server on Client Enablement Services. For more information, see Adding Voice Messaging servers on page 55.
4. If you are using an IMAP connection,
   a. set **IMAP4 Super User Access Allowed** field to **yes**.
   b. if you are using SSL, set **IMAP4 Super User Connection Security** field to **Must use SSL or encrypted SASL**.
5. If you are using an LDAP connection,
   a. set **LDAP Access Allowed** field to **yes**.
   b. depending on the LDAP connection you are using, set **LDAP Connection Security** field to **Must use SSL or encrypted SASL** if you are using SSL port 636, or set to **No Encryption required** if you are using port 389.
6. Click **Save**.

Configuring Communication Manager Messaging for Avaya one-X® Client Enablement Services

Configuring Communication Manager Messaging ports and protocols

About this task

If you change the default ports for one or more of these protocols in Communication Manager Messaging, you must change the default settings in the Avaya one-X® Client Enablement Services Administration application.

Note:

Client Enablement Services integrates with messaging servers using only the Avaya message store, and not any other e-mail message stores.

Procedure

1. On the Communication Manager Messaging administration screen, go to **Messaging Administration** > **System Administration**.
2. On the Administer System Attributes and Features page, in the **System TCP/IP Ports** section, enable the following protocols:
   - **IMAP4 Port**
   - **SMTP Port**
   - **LDAP Port**
3. Validate the port numbers configured for these protocols against the port requirements for Client Enablement Services.

Verifying Communication Manager Messaging subscriber values

About this task

For every Avaya one-X® Client Enablement Services user, the mailbox number of the subscriber in Communication Manager Messaging must match the corresponding value in the Corporate Directory record for the user. If this value does not match, Client Enablement Services cannot accurately link incoming and outgoing communications with the correct users.

Procedure

1. In the Communication Manager Messaging administration screen, go to **Messaging Administration** > **Subscriber Management**.
2. On the Manage Subscribers page, click **Manage** adjacent to the machine name that hosts the subscribers.

   The subscribers can either be local subscribers or remote subscriber depending on the Communication Manager Messaging setup in your organization.
   - For local subscribers, on the Manage Local Subscribers page, verify if the mailbox number of the user matches the corresponding value in the user record in the Corporate Directory.
   - For remote subscribers, on the Manage Remote Subscribers page, verify if the mailbox number of the user matches the corresponding value in the user record in the Corporate Directory.

Establishing trusted connection between the Communication Manager Messaging server and the Client Enablement Services server

About this task

You should add Client Enablement Services in the trusted server list on the Communication Manager Messaging server so that they can connect using IMAP and LDAP protocols. Add a trusted link for each protocol as per the environment setup.

You must establish a trusted connection on the Communication Manager Messaging server for each Client Enablement Services server in the system.

Procedure

1. Go to **Server Administration** > **Trusted Servers**.
2. On the Manage Trusted Servers page, click **Add a new trusted server**.
3. On the Add Trusted Server page, enter the IP address of the Client Enablement Services server in the **IP Address** field, a **Trusted Server Name**, and a **Password**.

   Note:

   You should use the same login ID and password you used when adding a Voice Messaging server on Client Enablement Services. For more information, see Adding Voice Messaging servers on page 55.
4. If you are using an IMAP connection,
   a. set **IMAP4 Super User Access Allowed** field to **yes**.
   b. if you are using SSL, set **IMAP4 Super User Connection Security** field to **Must use SSL or encrypted SASL**.
5. If you are using an LDAP connection,
   a. set **LDAP Access Allowed** field to **yes**.
   b. depending on the LDAP connection you are using, set **LDAP Connection Security** field to **Must use SSL or encrypted SASL** if you are using SSL port 636, or set to **No Encryption required** if you are using port 389.
6. Click **Save**.

Configuring Avaya Aura® Conferencing for Avaya one-X® Client Enablement Services

Enabling Conferencing bridge features

Procedure

1. Enable the following Conferencing settings:

   a. ANI. Verify that Conferencing is configured to provide ANI (Caller ID) to identify meeting participants.

      This is configured by the `UriToTelnum.tab` file located at `/usr/ipcb/config/UriToTelnum.tab`. This is generally configured and working by default.

   b. Music. Verify that the music is available on Conferencing.

      The music setting is also enabled and configured by default. The music files are located in `/usr2/annun`. They are labeled as music_source1, music_source2, music_source3, music_source4.

2. (Optional) Enable the PINs setting and verify that support for PINs is available on Conferencing.

   Note:

   This is an optional feature and is enabled only if the customer wants to use unique PINs. By default, the system is set to accept moderator and participant codes.

3. Enable the following features required for Communication Manager to Conferencing connectivity:

   a. SIP trunk set. Verify that calls from Communication Manager to Conferencing provide Caller ID and DNIS correctly.

      The SIP trunk set is enabled by default unless you manually turn it off. The SIP trunk set is in the trunk setting on page 3. The Numbering Format should be set to **`public`**.

   b. DTMF. Verify that in-band/out-band DTMF in Communication Manager and Conferencing match and Conferencing receives DTMF properly.

      The DTMF setting is in the signaling group settings on page 1. DTMF over IP should be set to **`rtp-payload`**.

4. Enable the Dial feature and verify that Dial from Conferencing to Communication Manager is enabled and properly configured. To enable dialout perform one of the following:

a. For Meeting Exchange Release 5.2, insert a record in `/usr/ipcb/config/telnumToUri.tab` file where column values are:

   - TelnumPattern = *
   - TelnumConversion = *sip:$0@135.122.32.134:5060;transport=tcp*
   - Comment = *A comment*

   Replace the IP address in the TelnumConversion column with the CLAN or Processor Ethernet IP to allow dialout.

b. For Avaya Aura Conferencing Release 6.0, set the **Telnum to URI mappings** in the **Conferencing** > **Audio Conferencing** > **Call Routing** section in System Manager.

   See *Administering System Manager Release 6.0* for detailed information.

Configuring bridge operators for Conferencing

Procedure

1. Log in the Conferencing system as a root user.
2. Navigate to the **Flex-DAPI (FDAPI) Configuration** menu and configure the following settings:
   a. **Operators**. Set for 2 plus the number of operators required for Bridge Talk.
   b. **Music**. Define a music source.
3. Use the command **`dcbmaint`** to access the **System Maintenance Main Menu**.
4. Select the **Administrator Menu**.
5. Under the **System Administration Main Menu** options, select **System Sign-In Management**.
6. Under the **System Sign-In Management** menu options, select **Create Operator Sign-In**.
7. In the **Create Operator Sign-In** page, enter a **Sign-In Name**, **Password**, and **Telephone Number** for the operator.
8. Repeat steps 3 to 7 to create a sign-in for the second operator.

Configuring communication between Conferencing and Communication Manager

About this task

After you complete the standard Conferencing configuration for Communication Manager, you must ensure that the path from Conferencing to Communication Manager is properly set. Avaya one-X® Client Enablement Services requires this communication path to add a new participant into an ongoing conference.

Procedure

Verify that the `/usr/ipcb/config/telnumToUri.tab` file routes from Conferencing to Communication Manager.

Configuring on-demand conferences for PIN prompting (Optional)

About this task

If you want to enforce PIN identity for conferences, you must configure the individual PINs in PIN Code Administration 2.0. For more information, see the Conferencing documentation.

You can configure on-demand conferences for PIN prompting in one of the following ways:

- With a specific PIN list that you generate with PIN Administrator software
- With a value of ANYPIN that allows a user to enter any PIN value

Note:

You must configure Conferencing to provide Avaya one-X® Client Enablement Services with the values for moderator code, participant code, and PIN relative to the configuration of user resources.

Procedure

1. In the CRS system, navigate to the Customer Bookings window.
2. Create a new client.
3. Complete or enable the following values for the new client:
    - Participants
    - Demand
    - Conference PIN
    - Moderator PIN

- Reservation details
- Conference options for Music Source, Moderator Hang-Up, Security, and PIN options.

Configuring the Presence Services server for Avaya one-X® Client Enablement Services

Avaya one-X® Client Enablement Services and Presence Services certificate management overview

The WebSphere Application Server (WAS) of Avaya one-X® Client Enablement Services and Presence Services server obtain their personal certificates from the System Manager Certificate Authority signed certificates through the System Manager's Trust Management Interface. Client Enablement Services stores its personal certificate in the WAS NodeDefaultKeyStore and Presence Services stores its certificate in its keystore. Both Client Enablement Services and Presence Services store the CA signer certificate of System Manager in their trust stores. The CA signer certificate of System Manager is also obtained through the System Manager's Trust Management Interface. For example, Client Enablement Services stores System Manager signer certificate in the signer certificates of the NodeDefaultKeyStore. Therefore, you must make sure that both Presence Services and Client Enablement Services connect to the same System Manager, so that their personal certificates are signed by the same System Manager Certificate Authority.

When a secure connection is established between Client Enablement Services and Presence Services, they present their System Manager CA signed personal certificate to each other. Each of them accepts the personal certificate as valid because the certificate is signed by the same System Manager CA, which they have also stored in their trust stores.

After validating the Client Enablement Services certificate, Presence Services checks if the Client Enablement Services is authorized. For this, Presence Services checks if the FQDN of Client Enablement Services is in the trusted host list of Presence Services.

Configuring the Presence Services server for Avaya one-X® Client Enablement Services

Procedure

1. Log in to the Presence Services XCP Controller Web interface.
2. Select the **Advanced** configuration view.
3. Add each of the Avaya one-X® Client Enablement Services host names to the Trusted TLS host names. Perform the following steps:
    a. On the Presence Services XCP Controller main page, click **Edit** next to **Global Routing Settings**.
    b. On the Global Settings Configuration page, scroll down to the **Mutually Trusted TLS Hostnames** section and enter the host names in the **Host Filters** text box.

    The host names must match the CN value obtained from the Client Enablement Services personal certificate from WAS.

    Note:

    To obtain the CN name from WAS, select **Security** > **SSL certificate and key management** > **Key stores and certificates** > **NodeDefaultKeyStore** > **Personal certificates**. Enter the FQDN of the Client Enablement Services machine.

    The alias of the Client Enablement Services personal certificate is 1xkey.
4. Enter the details for AES Collector:
    a. On the Presence Services XCP Controller main page, click **Edit** next to **AES Collector**.
    b. On AES Collector Configuration page, scroll down to the **AES Collector Component** section.
    c. Enter **Default AES Username**. For example, `admin_login`.
    d. Enter **Default AES Password**. For example, `admin1_password`.
5. Enter the details for RTC Collector:
    a. On the Presence Services XCP Controller main page, click **Edit** next to **RTC Collector**.
    b. On the RTC Collector Configuration page, scroll down to the **Hostnames for this Component** section and enter **Host(s)**.
    c. On the RTC Collector Configuration page, scroll down to the **RTC Collector Component** section and enter **User Name**.

Note:

RTC collector is required only for OCS integration with Presence Services. For more details, see *Implementing Avaya Aura® Presence Services*.

6. To change the PostgresSQL settings in the Presence Services, perform these steps.
    1. Log in the Presence Services server CLI .
    2. Open the data directory using the command: **`cd /var/lib/pgsql/data`**
    3. In the data directory, use the **vi pg_hba.conf** command to modify the `pg_hba.conf` file and add the exact IP address ranges with proper masking bit at the end of the file. For example, `host all all <IP address of the Client Enablement Services server>/32 md5`.
    4. In the data directory, use the **vi postgresql.conf** command to modify the `postgresql.conf` file and set **listen_addresses = '*'**.
    5. Restart the postgres sql service using the command: **`service postgresql restart`**

Related topics:

User management on System Manager for enabling presence for Client Enablement Services users on page 276

Setting up System Manager for presence on page 279

Configuring System Manager for Avaya one-X® Client Enablement Services

System Manager integration overview

You must configure System Manager to manage Avaya Aura® Presence Services and Session Manager.

Creating SIP Entity for Client Enablement Services

Procedure

1. On the System Manager console, select **Routing** > **SIP Entities**.
2. Click **New**.

3. Enter the name of the Client Enablement Services server in the **Name** field.
4. Enter the FQDN or IP address of the Client Enablement Services server in the **FQDN or IP Address** field.
5. Select **SIP Trunk** in the **Type** drop-down menu.
6. Enter any other required information in the **Notes** field.
7. Enter the amount of time Session Manager should wait for a response from Client Enablement Services server in the **SIP Timer B/F** field.
8. In the **SIP Link Monitoring** drop-down menu, select one of the following:
   - **Link Monitoring Enabled** to enable SIP Link Monitoring
   - **Link Monitoring Disabled** to disable SIP Link Monitoring
9. Enter a value in **Proactive cycle time** field.

   This value specifies how often Session Manager monitors the entity when a link to the entity is up or active. Enter a value between 120 and 9000 seconds.
10. Enter a value in **Reactive cycle time** field.

    This value specifies how often Session Manager monitors the entity when a link to the entity is down or inactive. Enter a value between 30 and 900 seconds.
11. Enter a value in **Number of Retries** field.

    This specifies the number of times Session Manager tries to ping or reach the SIP entity before marking it as down or unavailable. Enter a value between 0 and 15.
12. To save the SIP entity, click **Commit**.

Creating Entity Link for Avaya one-X® Client Enablement Services

About this task

Configure an entity link between Session Manager and the Client Enablement Services server to send or receive messages between them.

Procedure

1. On the System Manager console, select **Routing** > **Entity Links**.
2. Click **New**.
3. Enter the name in the **Name** field.
4. Select the required Session Manager from the **SIP Entity 1** drop-down list.
5. Select **TCP** or **TLS** from the **Protocol** drop-down list.
6. Enter the port for SIP Entity 1.

   The default port for TCP is 5060 and for TLS is 5061.

Use the same protocol, either TCP or TLS, that is being used between Communication Manager and Session Manager.

7. Select the SIP Entity you created for Client Enablement Services from the **SIP Entity 2** drop-down list.
8. Enter the port for SIP Entity 2.

   The default port for TCP is 5060 and for TLS is 5061.

   Use the same protocol, either TCP or TLS, that is being used between Communication Manager and Session Manager.
9. Select the **Trusted** check box.
10. Click **Commit**.
11. To verify the SIP Entity link status, perform the following steps:
    a. Navigate to **Elements** >**Session Manager** > **System Status** > **SIP Entity Monitoring**.
    b. Under **All Monitored SIP Entities**, click the SIP Entity name you created for Session Manager and Client Enablement Services.
    The **Connection** and **Link Status** must be **up**.

Creating SIP Entity for Communication Manager

Before you begin

Before you create a SIP entity for Communication Manager, you must first check if there is an existing a SIP entity. If yes, then do not create a new SIP entity.

Procedure

1. On the System Manager console, select **Routing** > **SIP Entities**.
2. Click **New**.
3. Enter the name of the Communication Manager in the **Name** field.
4. Enter the FQDN or IP address of the Communication Manager in the **FQDN or IP Address** field.
   The FQDN should be either CLAN or procr IP.
5. Select **Communication Manager** in the **Type** drop-down menu.
6. Enter any other required information in the **Notes** field.
7. Enter the amount of time Session Manager should wait for a response from Communication Manager in the **SIP Timer B/F** field.
8. In the **SIP Link Monitoring** drop-down menu, select one of the following:
   - **Link Monitoring Enabled** to enable SIP Link Monitoring

- **Link Monitoring Disabled** to disable SIP Link Monitoring

9. Enter a value in **Proactive cycle time** field.

   This value specifies how often Session Manager monitors the entity when a link to the entity is up or active. Enter a value between 120 and 9000 seconds.

10. Enter a value in **Reactive cycle time** field.

    This value specifies how often Session Manager monitors the entity when a link to the entity is down or inactive. Enter a value between 30 and 900 seconds.

11. Enter a value in **Number of Retries** field.

    This specifies the number of times Session Manager tries to ping or reach the SIP entity before marking it as down or unavailable. Enter a value between 0 and 15.

12. To save the SIP entity, click **Commit**.

Creating Entity Link for Communication Manager

Before you begin

Before you create a Entity Link for Communication Manager, you must first check if there is an existing Entity Link. If yes, then do not create a new Entity Link.

About this task

Configure an entity link between Session Manager and Communication Manager to send or receive messages between them.

Client Enablement Services can connect to Communication Manager through Session Manager only when you create a SIP signaling group and trunk group is set between Communication Manager and Session Manager.

Procedure

1. On the System Manager console, select **Routing** > **Entity Links**.
2. Click **New**.
3. Enter the name in the **Name** field.
4. Select the required Session Manager from the **SIP Entity 1** drop-down list.
5. Select **TCP** or **TLS** from the **Protocol** drop-down list.
6. Enter the port for SIP Entity 1.

   The default port for TCP is 5060 and for TLS is 5061.
7. Select the SIP Entity you created for Communication Manager from the **SIP Entity 2** drop-down list.

   This should be the Communication Manager integrated with Client Enablement Services.

8. Enter the port for SIP Entity 2.
   The default port for TCP is 5060 and for TLS is 5061.
9. Select the **Trusted** check box.
10. Click **Commit**.

User management on System Manager for enabling presence for Client Enablement Services users

Client applications can use the presence functionality, only when you configure users on System Manager and add a presence resource to the user in Client Enablement Services.

Perform the following steps:

- Manage a user profile on System Manager
- Create a system presence ACL

Related topics:

Configuring the Presence Services server for Avaya one-X Client Enablement Services on page 271
Managing a user profile on System Manager on page 276
Creating a System Presence ACL on page 278
Managing users on page 279

Managing a user profile on System Manager

Procedure

1. On the System Manager console, go to **Users** > **Manage Users**.
2. In the User Management page > **Users** section, select the check box adjacent to a user, and click **Edit**.
3. In the **General** section, enter the **Last Name** and **First Name** of the user.
4. In the **Identity** section, perform the following:
   a. Enter a **Login** name.
      You must use the same login name for a user on System Manager, Active Directory, and Client Enablement Services. If you use different login names, this creates problem with presence status on client applications. System Manager displays the login name in small letters even if you use capital letters for the login name in the Active directory. Therefore, you should use small letters for the login name to avoid any problem.

   b. Select **Enterprise** from the **Authentication Type** drop-down list.
   c. Type a password for the System Manager in the **Password** field and confirm it in the **Confirm Password** field.
   d. Enter the **Localized Display Name** of the user.

      This is the name that is displayed as the calling party.
   e. Enter the full text name of the user for **Endpoint Display Name**.
   f. Select a language from the **Language Preference** drop-down list.
   g. Select a time zone from the **Time Zone** drop-down list.

5. Click the show or hide button for **Communication Profile**.
   a. By default, the **Name** field is pre-filled with the name of the user from the Active Directory.
   b. Select the **Default** check box to make the communication profile as the active profile.
   c. In the **Communication Profile Password** field, enter the password. This password must be same as the password set for the extension of the user on Communication Manager.
6. Click the show or hide button for **Communication Address**.
   a. Click **New**.
   b. Enter *Avaya SIP* in the **Type**.
   c. Enter the **Handle** and the **Domain**.

   The *Avaya SIP* communication address is required only for users who have a SIP extension.

   The Jabber communication address is created by default when the user is pulled from the LDAP during the synchronization performed on System Manager.
7. Click the show or hide button for **Session Manager Profile**.

   Session Manager profile is required only for users who have a SIP extension.
   a. Select a **Primary Session Manager**.
   b. Select a **Home Location**.
8. Select the **Endpoint Profile** check box to view the endpoint profile fields.

   Endpoint profile is required for users with either H.323 or SIP extensions.
   a. Select the Communication Manager on which you need add an endpoint from the **System** drop-down list.
   b. Select the **Use Existing Endpoints** check box.

      Note:

      Do not select the **Use Existing Endpoints** check box, if the extension of the user does not exist on Communication Manager.
   c. Click the icon in the **Extension** field, and select the extension of the end point you want to associate.

  d. Select a template you want to associate with the end point from the **Template** drop-down list.

     When you select a template, the system populates the corresponding set types. This is the set type of the endpoint you want to associate.

  e. Click the icon in the **Port** field to select a relevant port for the set type you select.

     This field lists the possible ports based on the selected set type.

9. Click the show or hide button for **Roles**.
   a. Select **End-User** from the list of **Available Roles**.
   b. Click **Assign Roles**.
10. Click **Commit**.

Creating a System Presence ACL

Procedure

1. On the System Manager console, go to **Users** > **System Presence ACLs**.
2. On the Presence ACL page, click the show/hide button next to **System Rule**.
3. In the **System Rule** section, click **New**.
4. Set **Priority** as **High**, **Access Level** as **All**, and **Action** as **Allow**.
5. Click **Commit**.
6. Click **New**.
7. Set **Priority** as **Low**, **Access Level** as **All**, and **Action** as **Allow**.
8. Click **Commit**.
9. In the **Default Policy** section, click **New**.
10. Set **Access level** as **All** and **Action** as **Allow**.
11. Click the show/hide button next to **System ACL** and click **New**.
12. In the **System ACL** section, click **New**.
13. On the New System ACL page, in the **Define Policy** section, click **New**.
    a. Set **Access Level** as **All**.
    b. Set **Action** as **Allow**.
    c. Click **Save**.
14. In the **Select Watcher** section, select all the users you want to add as a watcher.
15. Click **Commit**.

For more information of creating and managing ACL, see *Administering Avaya Aura System Manager* guide.

Next steps

Add a presence resource to the user.

For more information, see Assigning a Presence resource to a user on page 118.

Managing users

Procedure

1. Configure the LDAP on the System Manager.
2. Synchronize the LDAP with the System Manager so that users are imported.
3. Configure the user on the System Manager for its corresponding endpoint and telephony server.
4. Ensure that the **IP Softphone** option is selected for the user in the **Endpoint Properties** section.
5. In case of a SIP user, ensure that the value in the **Type of 3PCC Enabled** field is set to **Avaya**.

Setting up System Manager for presence

About this task

In Client Enablement Services, presence is handled by System Manager. Presence feature is enabled for only those users who are defined on System Manager. These users can be called as superset of the users defined on Client Enablement Services. Therefore, you can see presence for a contact not defined in Client Enablement Services only if this contact is defined as a user in System Manager.

Procedure

1. Set presence rules. See Setting Presence rules on page 280.
2. Create a System Presence ACL. See Creating a System Presence ACL on page 278.

3. Configure access level for presence. See Configuring Presence access level on page 280.

Related topics:

Configuring the Presence Services server for Avaya one-X Client Enablement Services on page 271

Setting Presence rules on page 280

Configuring Presence access level on page 280

Setting Presence rules

Procedure

1. On the System Manager console, click **Elements** > **Presence** > **Configuration**.
2. On the Presence page, in the **Presence Configuration Properties** table, click **Edit**.
3. Enter values for **Domain Substitution - From** and **Domain Substitution - To** fields.

   The **Domain Substitution - From** field value must be same as the domain name.

   The **Domain Substitution - To** field value is by default set to `pres.ips.avaya.com`. You can change this value if the value is different in the Presence Services system.
4. Click **Save**.

Configuring Presence access level

About this task

In System Manager, you can configure the Presence access level to **All** or **Telephony**.

- If you set the access level to **All**, the watcher can see all presence related information of the presentity.
- If you set the access level to **Telephony**, you can limit the level of presence information a watcher can have of the presentity.

To exchange presence information between client applications, you have to select **Avaya Application** from the list of **Available classes**. By default, the selected class in **Telephony** is **Phone**.

Procedure

1. On the System Manager console, click **Elements** > **Presence** > **Access Levels**.
2. On the Presence page, select **Telephony** in the Presence Access Levels section.
3. Click **Edit**.
4. In the Edit Presence Access Level section, select **Avaya Application** in the **Available Classes** list.
5. Click the single right arrow (>) to move the **Avaya Application** class to the list of **Selected Classes**.
6. Click **Save**.

Related topics:

Configuring the Presence Services server for Avaya one-X Client Enablement Services

Presence Services server on page 63

Configuration worksheets for integrated servers

Configuration worksheet for Session Manager

This worksheet lists the information you need to configure Session Manager for Avaya one-X® Client Enablement Services. You need these values to configure the Auxiliary server in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Handle	smhandle		The unique name assigned to the server by the administrator. You must create this value in the Administration application.
Description	Chicago SM		A short description of the server that uniquely identifies the Session Manager. You must create this value in the Administration application.
Domain	sysucd.avaya.com		This is the domain to which the System Manager belong or is configured.

Property name	Property values		Notes
	Example value	Your value	
SIP Address Host	192.168.1.174		IP address of the asset card configured in the Session Manager.
SIP Address Port	5060		The port used by the Session Manager to talk to the Client Enablement Services server. This value is not available in Session Manager. You must create this value in the Administration application.

Configuration worksheet for Communication Manager

This worksheet lists the information that you need to configure Communication Manager for Avaya one-X® Client Enablement Services. You need these values to configure the Communication Manager services in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Handle	cmhandle		The unique name assigned to the server by the administrator. You must create this value in the Administration application.
Description	Chicago CM PBX		A short description of the server that uniquely identifies the Telephony server. You must create this value in the Administration application.
SIP Remote Host	###.###.###.###		SIP remote host is a Communication Manager Ethernet interface that is configured as the Near-end node in the Communication Manager signaling group configuration to communicate with Client Enablement Services server. **Note:** If you configure Communication Manager as Processor Ethernet (PE), enter the IP address of the PROCR

Property name	Property values		Notes
	Example value	Your value	
			interface of Communication Manager.
SIP Remote Port			The port used by Communication Manager to talk to the Client Enablement Services server.
Dial Plan	dialplanhandle		The handle of the Dial Plan used by this server.

Configuration worksheet for Modular Messaging

This worksheet lists the information that you need to configure Modular Messaging for Avaya one-X® Client Enablement Services. You need these values to configure the Voice Messaging server in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Handle	mmhandle		The unique name assigned to the server by the administrator. You must create this value in the Administration application.
Description	Chicago MM Server		A short description of the server that uniquely identifies the Voice Messaging server. You must create this value in the Administration application.
Initial Number of Server Connections	50		The minimum number of Client Enablement Services user connections needed to communicate with the storage server of the messaging server. This value is not available in Modular Messaging. You must create this value in the Administration application.
Client Connections Increment	2		The number of times to increment the connections based on the number of users in the connections. For example, if this value is 2 and there are 100 users per connection, the connections increments for every 200 users.

Property name	Property values		Notes
	Example value	Your value	
			This value is not available in Modular Messaging. You must create this value in the Administration application.
Users Per Client Connection	10		The number of users assigned per connection to the Voice Messaging server. This value is not available in Modular Messaging. You must create this value in the Administration application.
Messages Temp Directory	/tmp or / msgWorkDir		The location of the temporary directory where sections of voice mail message are stored. When creating a new Voice Messaging server, enter either the name of the default directory `/msgWorkDir` or the name of the directory you created for the Voice Messaging server. This value is not available in Modular Messaging. You must create this value in the Administration application.
Temp Purge Interval	60		The number of minutes that the sections of voice mail messages can remain in storage before the temporary directory is purged and the sections are deleted. This value is not available in Modular Messaging. You must create this value in the Administration application.
Mail Domain	server.xyzcorp .com		The fully qualified domain name of the storage server of the messaging server.
Dial Plan	dialplanhandle		The handle of the Dial Plan used by this server.
IMAP Host	###.###.###.# ##		The network address of the storage server of the messaging server. This field must include an IP address, not a fully qualified domain name.

Property name	Property values		Notes
	Example value	Your value	
IMAP Port	993		The secure port number used by the **IMAP** configuration for the Voice Messaging server.
IMAP Login ID	oneXPIMAP		The secure log-in ID used by the **IMAP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
IMAP Password			The secure password associated with the log-in ID used by the **IMAP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in your Voice Messaging server.
IMAP Secure Port	Yes		If you select this option, Client Enablement Services requires a secure **IMAP** connection for the Voice Messaging server. Verify that this port is the correct port for a secure connection.
SMTP Host	###.###.###.###		The network address of the storage server of the messaging server.
SMTP Port	25		The port number used by the **SMTP** configuration for the Voice Messaging server.
SMTP Login ID	IMAP4		The secure log-in ID used by the **SMTP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
SMTP Password			The secure password associated with the log-in ID used by the **SMTP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted**

Property name	Property values		Notes
	Example value	Your value	
			Server Name in the Voice Messaging server.
SMTP Secure Port	Yes		If selected, indicates **SMTP** is configured to use a secure connection for the Voice Messaging server. A secure **SMTP** connection to the Voice Messaging server is optional.
LDAP Host	###.###.###.###		The network address of the storage server of the messaging server. This field must include an IP address, not a fully qualified domain name.
LDAP Port	636		The port number used by the **LDAP** configuration for the Voice Messaging server.
LDAP Login ID	oneXPLDAP		The log-in ID used by the **LDAP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
LDAP Password			The password associated with the log-in ID used by the **LDAP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in the Voice Messaging server.

Configuration worksheet for Messaging

This worksheet lists the information you need to configure Messaging for Avaya one-X® Client Enablement Services. You need these values to configure the Voice Messaging server in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Handle	mhandle		The unique name assigned to the server by the administrator. You must create this value in the Administration application.
Description	Chicago Messaging Server		A short description of the server that uniquely identifies the Voice Messaging server. You must create this value in the Administration application.
Initial Number of Server Connections	50		The minimum number of Avaya one-X® Client Enablement Services connections needed to communicate with the Voice Messaging server, the Storage server of the Messaging server. This value is not available in Messaging. You must create this value in the Administration application.
Client Connections Increment	2		The number of times to increment the connections based on the number of users in the connections. For example, if this value is 2 and there are 100 users per connection, the connections increments for every 200 users. This value is not available in Messaging. You must create this value in the Administration application.
Users Per Client Connection	10		The number of users assigned per connection to the Voice Messaging server. This value is not available in Messaging. You must create this value in the Administration application.
Messages Temp Directory	/tmp or /msgWorkDir		The location of the temporary directory where sections of voice mail message are stored. when creating a new Voice Messaging server, enter either the name of the default directory /msgWorkDir or the name of the

Property name	Property values		Notes
	Example value	Your value	
			directory you created for the Voice Messaging server. This value is not available in Messaging. You must create this value in the Administration application.
Temp Purge Interval	60		The number of minutes that the sections of voice mail messages can remain in storage before the temporary directory is purged and the sections are deleted. This value is not available in Messaging. You must create this value in the Administration application.
Mail Domain	server.xyzcorp .com		The fully qualified domain name of the Storage server of the Messaging server.
Dial Plan	dialplanhandle		The handle of the Dial Plan used by this server.
IMAP Host	###.###.###.# ##		The network address of the Storage server of the Messaging server. This field must include an IP address, not a fully qualified domain name.
IMAP Port	993		The secure port number used by the **IMAP** configuration for the Voice Messaging server.
IMAP Login ID	oneXPIMAP		The secure log-in ID used by the **IMAP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
IMAP Password			The secure password associated with the log-in ID used by the **IMAP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in your Voice Messaging server.

Property name	Property values		Notes
	Example value	Your value	
IMAP Secure Port	Yes		If you select this option, Client Enablement Services requires a secure **IMAP** connection for the Voice Messaging server. Verify that this port is the correct port for a secure connection.
SMTP Host	###.###.###.###		The network address of the Storage server of the Messaging server.
SMTP Port	25		The port number used by the **SMTP** configuration for the Voice Messaging server.
SMTP Login ID	IMAP4		The secure log-in ID used by the **SMTP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
SMTP Password			The secure password associated with the log-in ID used by the **SMTP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in the Voice Messaging server.
SMTP Secure Port	Yes		If selected, indicates **SMTP** is configured to use a secure connection for the Voice Messaging server. A secure **SMTP** connection to the Voice Messaging server is optional.
LDAP Host	###.###.###.###		The network address of the Storage server of the Messaging server. This field must include an IP address, not a fully qualified domain name.
LDAP Port	636		The port number used by the **LDAP** configuration for the Voice Messaging server.

Property name	Property values		Notes
	Example value	Your value	
LDAP Login ID	oneXPLDAP		The log-in ID used by the **LDAP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
LDAP Password			The password associated with the log-in ID used by the **LDAP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in the Voice Messaging server.

Configuration worksheet for Communication Manager Messaging

This worksheet lists the information you need to configure in the Communication Manager Messaging server for Avaya one-X® Client Enablement Services. You need these values to configure the Voice Messaging server in the Avaya one-X® Client Enablement Services Administration application.

Property name	Property values		Notes
	Example value	Your value	
Handle	cmmhandle		The unique name assigned to the server by the administrator. You must create this value in the Administration application.
Description	Chicago Messaging Server		A short description of the server that uniquely identifies the Voice Messaging server. You must create this value in the Administration application.
Initial Number of Server Connections	50		The minimum number of Avaya one-X® Client Enablement Services connections needed to communicate with the Voice Messaging server, the storage server of the Communication Manager Messaging server.

Property name	Property values		Notes
	Example value	Your value	
			This value is not available in Communication Manager Messaging. You must create this value in the Avaya one-X® Client Enablement Services Administration application.
Client Connections Increment	2		The number of times to increment the connections based on the number of users in the connections. For example, if this value is 2 and there are 100 users per connection, the connections increments for every 200 users. This value is not available in Communication Manager Messaging. You must create this value in the Avaya one-X® Client Enablement Services Administration application.
Users Per Client Connection	10		The number of users assigned per connection to the Voice Messaging server. This value is not available in Communication Manager Messaging. You must create this value in the Administration application.
Messages Temp Directory	/tmp or / msgWorkDir		The location of the temporary directory where sections of voice mail message are stored. when creating a new Voice Messaging server, enter either the name of the default directory `/tmp/msgWorkDir` or the name of the directory you created for the Voice Messaging server. This value is not available in Communication Manager Messaging. You must create this value in the Administration application.
Temp Purge Interval	60		The number of minutes that the sections of voice mail messages can remain in storage before the

Property name	Property values		Notes
	Example value	Your value	
			temporary directory is purged and the sections are deleted. This value is not available in Communication Manager Messaging. You must create this value in the Administration application.
Mail Domain	server.xyzcorp .com		The fully qualified domain name of the storage server of the Communication Manager Messaging server.
Dial Plan	dialplanhandle		The handle of the Dial Plan used by this server.
IMAP Host	###.###.###.# ##		The network address of the storage server of the Communication Manager Messaging server. This field must include an IP address, not a fully qualified domain name.
IMAP Port	993		The secure port number used by the **IMAP** configuration for the Voice Messaging server.
IMAP Login ID	oneXPIMAP		The secure log-in ID used by the **IMAP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
IMAP Password			The secure password associated with the log-in ID used by the **IMAP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in your Voice Messaging server.
IMAP Secure Port	Yes		If you select this option, Client Enablement Services requires a secure **IMAP** connection for the Voice Messaging server. Verify that this port is the correct port for a secure connection.

Property name	Property values		Notes
	Example value	Your value	
SMTP Host	###.###.###.### ##		The network address of the storage server of the Communication Manager Messaging server.
SMTP Port	25		The port number used by the **SMTP** configuration for the Voice Messaging server.
SMTP Login ID	IMAP4		The secure log-in ID used by the **SMTP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
SMTP Password			The secure password associated with the log-in ID used by the **SMTP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in the Voice Messaging server.
SMTP Secure Port	Yes		If selected, indicates **SMTP** is configured to use a secure connection for the Voice Messaging server. A secure **SMTP** connection to the Voice Messaging server is optional.
LDAP Host	###.###.###.### ##		The network address of the storage server of the Communication Manager Messaging server. This field must include an IP address, not a fully qualified domain name.
LDAP Port	636		The port number used by the **LDAP** configuration for the Voice Messaging server.
LDAP Login ID	oneXPLDAP		The log-in ID used by the **LDAP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server**

Property name	Property values		Notes
	Example value	Your value	
			Name in your Voice Messaging server.
LDAP Password			The password associated with the log-in ID used by the **LDAP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in the Voice Messaging server.

Configuration worksheet for Conferencing

This worksheet lists the information that you need to configure Conferencing for Avaya one-X® Client Enablement Services. You need these values to configure the Conference services in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Handle	mxhandle		The unique name assigned to the server by the administrator. You must create this value in the Administration application.
Description	Chicago Conf Server		A short description of the server that uniquely identifies the Conferencing server. You must create this value in the Administration application.
BCAPI Logger Directory	/tmp		The path name of the directory where information about **BCAPI** issues is stored. See Creating a directory for the Conferencing server on page 59. This value is not available in Conferencing. You must create this value in the Administration application.
Dial Plan	Dialplan		The handle of the Dial Plan used by this server.
BCAPI Host	###.###.###.###		The network address that the **BCAPI** configuration uses for the

Property name	Property values		Notes
	Example value	Your value	
			Conferencing server as an IP address or a DNS address.
BCAPI Login ID	username1		The log-in ID that the **BCAPI** configuration uses for the Conferencing server.
BCAPI Password			The password associated with the log-in ID that the **BCAPI** configuration uses for the Conferencing server.
BCAPI Secondary Login ID	username2		The **Secondary Login ID** used by the **BCAPI** configuration for the Conferencing server.
BCAPI Password			The password associated with the **Secondary Login ID** used by the **BCAPI** configuration for the Conferencing server.

Configuration worksheet for Presence

This worksheet lists the information that you need to configure Presence for Avaya one-X® Client Enablement Services. You need these values to configure the Presence Services in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Type	apas		The type of server configured on the system. For the Presence Services displays apas.
Version	6.1		The version of the server configured on the system.
Handle	PS6.1		The unique name assigned to the server by the administrator. You must create this value in the Administration application.
Description	Chicago IPS Server		A short description of the server that uniquely identifies the Presence Services. You must create this value in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Enabled	Yes		When selected, enables the telephony server for the Client Enablement Services server.
PS Publish To Port	5061		The port number on the Presence Services server where the presence information of the user is published. This is a remote port.
PS Consumer Port	9072		The port number on the Presence Services server that receives the consumer information.
PS Supplier Port	9070		The port number on the Presence Services server that furnishes the published the information.
Web service Port	443		Web Services port used by the LPS when communicating with the System Manager.
RMI Export Port	2009		Replication listener is exported on the RMI export port. The exported objects are authorization request call-backs. On the Local Presence Services (LPS), the default value of the port is 0. This means that the system selects the available port.
RMI Registry Port	2009		RMI register listens on the RMI registry port. On LPS, the default value of the port is 2009.
RMI Secure Port			Select this check box to make the replication related RMI communication secure.
Presence Services (PS) Host	192.168.2.19		The network host address of Presence Services. It can be defined either as FQDN (fully qualified domain name), or as an IP address.
Presence Services (PS) Port	5061		The SIP service communication port between LPS and Presence Services.

Property name	Property values		Notes
	Example value	Your value	
Management Service (SMGR) Host	192.168.2.14		The network host address of . It can be defined either as FQDN or as an IP address.
Management Service (SMGR) Port	1399		TCP/IP port used for LPS to communicate with .
Management Service (SMGR) Login ID	admin		The log-in ID used by the for the presence server.
Management Service (SMGR) Password			The password associated with the log-in ID used by the for the presence server.
Confirm			Verification of the password associated with the log-in ID used by the for the presence server.

Configuration worksheet for Dial Plan

This worksheet lists the information that you need to configure a dial plan for Avaya one-X® Client Enablement Services. You need these values to configure the dial plan in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Handle	Dialplan		The unique name assigned to the server by the administrator. You must create this value in the Administration application.
Phone Numbers PBX Main	15555551234		A sample of a valid telephone number on the switch. The Dial Plan compares this number with other telephone numbers to determine whether a telephone number is internal or external.
Phone Numbers Automatic Routing Service	9		The digit to prefix before an outbound phone number is dialed on the PBX. For example, in the phone number 9-1-800-8888, 9 is the **Automatic Routing Service** number.

Property name	Property values		Notes
	Example value	Your value	
Prefixes Regional	1555		The area code of the region.
Prefixes Inter-Regional	1		The digit to dial between area codes in an **Inter-Regional** phone call.
Prefixes International	011		The digits to prefix to place an **International** phone call. For example, in the phone number 011-1-800-8888, 011 is the **International** prefix code.
Number of Digits National Call Maximum	10		The maximum number of digits allowed in a domestic telephone call. For example, if the phone number is 508-852-0010, the value is 10.
Number of Digits Local Call	7		The maximum number of digits in a telephone call within an area code. For example, if the phone number is 508-852-0010, the value is 10.
Number of Digits Extension to Extension Call	5		The maximum number of digits allowed in a phone extension at the enterprise. Typically, this value is 7 or less.

Chapter 11: Miscellaneous tasks

Restarting Client Enablement Services

Before you begin

To restart Client Enablement Services server, you must restart the Web Application server (WAS).

About this task

After you restart the Client Enablement Services server or any of its services, and if you get an error as `Error initialising the page` while trying to login to the Client Enablement Services administration application, you should close the Web browser and open a new browser and try accessing the administration application again.

You can reboot the Client Enablement Services server from either Avaya Aura® System Platform or using linux commands.

Procedure

1. To reboot the server from the System Platform, perform the following steps:
    a. Log in to System Platform.
    b. On the left pane, click **Virtual Machine Management** > **Manage**.
    c. On the Virtual Machine List page, click the link of the Client Enablement Services virtual machine.
    d. On the Virtual Machine Configuration Parameters page, click **Reboot**.
2. To reboot the server using linux commands, perform the following steps:
    a. SSH in to the Client Enablement Services terminal using Putty.
    b. On the shell prompt, type the **`service 1xp restart`** command to restart the Client Enablement Services service.
    The system prompts you to enter your username and password when it tries to stop the server.
    c. Enter your admin_user_name and the admin_user_password.
    This stops and restarts the Client Enablement Services server. If the server starts successfully, you get an output similar to as shown below:

```
# service 1xp restart
Stopping WebSphere Application Server - server1 ...
ADMU0116I: Tool information is being logged in file
 /opt/IBM/WebSphere/AppServer70/profiles/default/logs/server1/
stopServer.log
ADMU0128I: Starting tool with the default profile
```

```
ADMU3100I: Reading configuration for server: server1
Realm/Cell Name:<default>
Username:
Password:


ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server server1 stop completed.
Starting WebSphere Application Server - server1 ...
ADMU0116I: Tool information is being logged in file
/opt/IBM/WebSphere/AppServer70/profiles/default/logs/server1/
startServer.log
ADMU0128I: Starting tool with the default profile
ADMU3100I: Reading configuration for server: server1
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server server1 open for e-business; process id is 26491
```

Note:

During the service restart of Client Enablement Services if you enter an incorrect user name or password, the server stop fails. After failing to stop the server, the script tries to start the server and the system displays an error message: An `instance of the server may already be running: <server name>`.

Stopping Client Enablement Services

Procedure

1. SSH in to the Client Enablement Services server terminal using Putty.
2. On the shell prompt, type the **`service 1xp stop`** command to stop the Client Enablement Services service.
   The system prompts you to enter your username and password when it tries to stop the server.
3. Enter your admin_user_name and the admin_user_password.
   This stops the Client Enablement Services server. If the server stops successfully, you get an output similar to as shown below:

   ```
   # service 1xp stop
   Stopping WebSphere Application Server - server1 ...
   ADMU0116I: Tool information is being logged in file
    /opt/IBM/WebSphere/AppServer70/profiles/default/logs/server1/
   stopServer.log
   ADMU0128I: Starting tool with the default profile
   ADMU3100I: Reading configuration for server: server1
   Realm/Cell Name:<default>
   Username:
   Password:
   ```

```
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server server1 stop completed.
```

Starting Client Enablement Services

Procedure

1. SSH in to the Client Enablement Services server terminal using Putty.
2. On the shell prompt, type the **`service 1xp start`** command to start the Client Enablement Services service.
   This starts the Client Enablement Services server. If the server starts successfully, you get an output similar to as shown below:

```
# service 1xp start
Starting WebSphere Application Server - server1 ...
ADMU0116I: Tool information is being logged in file
/opt/IBM/WebSphere/AppServer70/profiles/default/logs/server1/
startServer.log
ADMU0128I: Starting tool with the default profile
ADMU3100I: Reading configuration for server: server1
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server server1 open for e-business; process id is 26491
```

Restarting Audio Transcoding server

Procedure

1. SSH in to the Client Enablement Services server terminal using Putty.
2. On the shell prompt, type the **`service transcoding_server restart`** command to restart the Audio Transcoding server.
   This stops and starts the Audio Transcoding server. If the server stops successfully, you get an output similar to as shown below:

```
# service transcoding_server restart
Restarting transcoding_server:
Stopping transcoding_server:                               [  OK  ]
Service is already running
Starting transcoding_server:                               [  OK  ]
```

Stopping Audio Transcoding server

Procedure

1. SSH in to the Client Enablement Services server terminal using Putty.
2. On the shell prompt, type the **`service transcoding_server stop`** command to stop the Audio Transcoding server.
   This stops the Audio Transcoding server. If the server stops successfully, you get an output similar to as shown below:

   ```
   # service transcoding_server stop
   Stopping transcoding_server:                                [  OK  ]
   ```

Starting Audio Transcoding server

Procedure

1. SSH in to the Client Enablement Services server terminal using Putty.
2. On the shell prompt, type the **`service transcoding_server start`** command to start the Audio Transcoding server.
   This starts the Audio Transcoding server. If the server starts successfully, you get an output similar to as shown below:

   ```
   # service transcoding_server start
   Starting transcoding_server:                                [  OK  ]
   ```

Restarting Handset server

Procedure

1. SSH in to the Client Enablement Services server terminal using Putty.

   Note:

   In a co-resident installation, you should log in to the Client Enablement Services server whereas in a standalone installation, you should log in to the Handset server.

2. On the shell prompt, type the **`service handset_server restart`** command to restart the Handset server.
   This stops and starts the Handset server. If the server stops successfully, you get an output similar to as shown below:

   ```
   # service handset_server restart
   Restarting handset_server:
   Please check the details in server.log
   Stopping handset_server:                                 [  OK  ]
   Starting handset_server:                                   [  OK  ]
   ```

   The server.log file is in`/opt/avaya/HandsetServer/logs`.

Stopping Handset server

Procedure

1. SSH in to the Client Enablement Services server terminal using Putty.

   Note:

   In a co-resident installation, you should log in to the Client Enablement Services server whereas in a standalone installation, you should log in to the Handset server.

2. On the shell prompt, type the **`service handset_server stop`** command to stop the Handset server.
   This stops the Handset server. If the server stops successfully, you get an output similar to as shown below:

   ```
   # service handset_server stop
   Please check the details in server.log
   Stopping handset_server:                               [  OK  ]
   ```

   The server.log file is in`/opt/avaya/HandsetServer/logs`.

Starting Handset server

Procedure

1. SSH in to the Client Enablement Services server terminal using Putty.

> **Note:**
>
> In a co-resident installation, you should log in to the Client Enablement Services server whereas in a standalone installation, you should log in to the Handset server.

2. On the shell prompt, type the **`service handset_server start`** command to start the Handset server.
   This starts the Handset server. If the server starts successfully, you get an output similar to as shown below:

   ```
   # service handset_server start
   Starting handset_server:                                [  OK  ]
   ```

   The server.log file is in`/opt/avaya/HandsetServer/logs`.

Restarting the IBM HTTP server

Procedure

1. Log in to the Client Enablement Services server CLI.
2. On the shell prompt, type the **`service ihs restart`** command to restart the HTTP server.

Stopping the IBM HTTP server

Procedure

1. Log in to the Client Enablement Services server CLI.
2. On the shell prompt, type the **`service ihs stop`** command to stop the HTTP server.

Starting the IBM HTTP server

Procedure

1. Log in to the Client Enablement Services server CLI.
2. On the shell prompt, type the **`service ihs start`** command to start the HTTP server.

Starting and stopping the database manually

You can connect to the database when you are not able to connect to the Avaya one-X® Client Enablement Services administration application. When you restart the Client Enablement Services server and you are not able to log in to the administration application, then you can connect to the database server to start the database.

Procedure

1. Log in to the Client Enablement Services server as root.
2. Type `su - dbinst` and press Enter.

   Here, `dbinst` is the name of the Client Enablement Services database server instance.
3. Type `db2start` and press Enter to start the database.

   You can use the `db2stop` command to stop the database.

Removing Client Enablement Services control on Communication Manager stations

About this task

You can remove the control of Client Enablement Services on Communication Manager for either one user or for all users. For example, you should remove the control on all stations if you want to change your hardware, but you should remove the control on only the user's station on Communication Manager when the user is not using the client application.

Removing the control on station for one or more users of Client Enablement Services system is important because one EC500 license and one PBFMC license are consumed per user extension when you assign a mobile telephony resource to the user on the Client Enablement Services system.

Procedure

1. To remove the control on stations for one user, perform the following:
    a. In the Client Enablement Services administration application, select the **Users** tab.
    b. From the left pane, select **Provisioned Users**.
    c. On the Provisioned Users page, search for the user using any of the search criteria.
    d. On the View User page, click **Disable** if the **State** of the user is **Enabled**.

    ✱ **Note:**

    When you assign a mobile telephony resource to a user, Client Enablement Services enables the extension of the user on Communication Manager for Also Ring, Call back, Call logging, Block all calls, and VIP calling features.
2. To remove the control on all stations for all users, perform the following:
    a. In the Client Enablement Services administration application, select the **Monitors** tab.
    b. In the left pane, select **Telephony**.
    The Monitor Telephony Services page displays the current run-time status for services on Client Enablement Services, such as Communication Manager and SIP.
    c. Click **Suspend** in the box displaying the SIP service adapter connected to the Communication Manager on which you have to remove the control of the Client Enablement Services system.

    If you click **Resume**, all control of the Client Enablement Services system are restored on the Communication Manager stations.

Creating a self-signed certificate on the IBM WebSphere

Certificates usually have a finite life. Before the certificate expires, you must renew the certificate by either creating a new self-signed certificate, or renew your third-party certificate with the Certificate Authority.

Procedure

1. Log in to the IBM console.
2. From the left navigation pane, select **Security** > **SSL certificate and key management**.
3. Perform the following procedure to create a self-signed certificate.
    a. On the SSL certificate and key management page, under **Related Items**, select **Key stores and certificates**.
    b. Select **NodeDefaultKeyStore**.
    c. Under **Additional Properties**, click **Personal certificates**.
    d. From the **Create** drop-down list, select **Chained certificate**.
    e. Enter details of the certificate such as Alias, Common name, Validity period, Organization, Organization unit, Locality, State/Province, Zip code, Country or Region.
    f. Click **Apply**.
    The system displays the certificate details such as Version, Key size, Serial number, validity period, Issue to, Issue by, Fingerprint, Signature algorithm.
    g. Click **Save directly to the master configuration**.
4. Perform the following procedure to make the new certificate the default certificate.
    a. Go to **SSL certificate and key management**.
    b. Under **Related Items**, click **SSL Configurations**.
    c. Click **NodeDefaultSSLSettings**.
    d. In the **Default server certificate alias** drop-down list, select the new certificate you created.
    e. In the **Default client certificate alias** drop-down list, select the new certificate you created, and click **Ok**.
    f. Click **Save directly to the master configuration**.
    g. Close the browser and start a new session for the changes to take effect.
5. (Optional) Perform the following procedure to delete the old certificate.
    a. Go to **SSL certificate and key management**.
    b. Under **Related Items**, click **Key stores and certificates**.
    c. Select **NodeDefaultKeyStore**.
    d. Under **Additional Properties**, click **Personal certificates**.
    e. Select the check box adjacent to the alias of the certificate you want to delete, and click **Delete**.
    f. Click **Save directly to the master configuration**.

Chapter 12: Troubleshooting

Troubleshooting the Administration application

This chapter lists few troubleshooting issues related to the administration application that you might encounter. Each troubleshooting topic briefly explains the problem, what caused the problem, if known, and the proposed solution. For a detailed list of all the known troubleshooting issues and their proposed solutions, see the *Troubleshooting Avaya one-X® Client Enablement Services* guide.

System Manager certificate is not imported after installation

If the System Manager certificate is not imported after Client Enablement Services installation or if there is any change in the System Manager Host or IP address, you should check the Presence Services server.

Proposed solution

About this task

Perform the following steps when the Presence Services is in running state.

Procedure

1. Ensure that the System Manager host and port details are included in the`/opt/avaya/1xp/config.properties` file.
   For example:
   ```
   smgr.host=135.9.2 x.xx
   smgr.port=443
   ```
2. Reassign the certificate from System Manager.
   a. In the SSH terminal session on the Client Enablement Services 6.1 server, log in as root.
   b. Go to `/opt/avaya/1xp` directory using the command: `cd /opt/avaya/1xp`

c. Renew the certificate using the command: `./run_config_smgr_jython.pl <smgr_enrollment_password>`

d. Restart the Client Enablement Services server.

3. Verify whether the System Manager and Presence Services server are reachable by the FQDN.
   If they are not reachable, add entries to `/etc/hosts`.

Unable to administer statistics table

When you enable collection for Performance statistics and Feature Usage statistics in the Client Enablement Services administration application, you must also schedule the cleanup settings for these statistics. If you do not schedule the cleanup settings, the statistics table becomes very large in size and it becomes impossible to administer the table.

If you forget to schedule the cleanup settings or the scheduler did not run and the statistics table has become very large in size, you can use a shell script to reset the statistics.

Proposed solution

Procedure

1. On the Client Enablement Services server, log in as a dbinst user.
2. Type `su - dbinst`.
3. Change directory to `/opt/avaya/1xP/`.
4. Enter the command **`./reset_stats.sh roinst`**
   This script cleans up all statistics data.

   Note:

   You should execute this script as a database instance user. This script receives the read only user name of the database as a parameter.

   On successful execution of the script, the output is similar to as below.

```
[dbinst@<machine_name> 1xp]$ ./reset_stats.sh roinst
Clean stats
Database Connection Information

 Database server        = DB2/LINUXX8664 9.7.0
 SQL authorization ID   = DBINST
 Local database alias   = ACPDB

DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.
```

```
DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.
DB20000I  The SQL DISCONNECT command completed successfully.
Set permissions on statistics for roinst
   Database Connection Information

 Database server        = DB2/LINUXX8664 9.7.0
 SQL authorization ID   = DBINST
 Local database alias   = ACPDB

DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.

DB20000I  The SQL DISCONNECT command completed successfully.
DB20000I  The TERMINATE command completed successfully.
```

Client Enablement Services user mapping is not in sync with Communication Manager

When you restart Communication Manager, the one-X mappings on Communication Manager are lost and features enabled by Client Enablement Services on extensions of users are disabled temporarily. However, when the link between Client Enablement Services and Communication Manager comes up, the user mappings are restored automatically on Communication Manager and all features are enabled.

The link comes up automatically in approximately 10 to 15 minutes, and this time depends on the number of users provisioned on the Client Enablement Services server.

Related topics:

Assigning a Mobile Telephony resource to a user on page 113

Proposed solution

About this task

If the mappings are not restored automatically, you should restart the Communication Manager service adapter from the Client Enablement Services administration application. Perform the following steps:

Procedure

1. Click the **Monitors** tab.
2. In the left pane, select **Telephony**.
3. In the section that displays the details of Communication Manager Service, click **Restart** in the **Action** box.

The system restarts the Communication Manager service adapter.

Unable to connect to Communication Manager

If the Client Enablement Services server is not able to connect to the Communication Manager system configured on the Client Enablement Services administration application after you make changes to the Trunk group or the Signaling group on Communication Manager, the system displays the following error:

```
CM XXX.XXX.XXX.XXX not accepting SIP messages from server
YYY.YYY.YYY.YYY
```

In this error message, *XXX.XXX.XXX.XXX* is the IP address of Communication Manager and *YYY.YYY.YYY.YYY* is the IP address of the Client Enablement Services server.

Proposed solution

Before you begin

Follow these steps only when the **Allow Direct Connection to CM** check box is selected on the **Servers** > **Telephony Servers** page in the Client Enablement Services administration application.

Procedure

1. Verify that the **Far-end domain** field value mentioned for the SIP signaling group on Communication Manager and the value mentioned in the **Domain** field for the SIP Local server on the Client Enablement Services administration application are same.
2. Verify that the **Far-end Listen Port** field value on Communication Manager and the value mentioned in the **Port** field for the SIP Local server on the Client Enablement Services administration application are same.
3. Verify that the **Near-end Listen Port** field value on Communication Manager and the value mentioned in the **SIP Remote Port** field for the Telephony server on the Client Enablement Services administration application are same.
4. Ensure that the protocol configured for SIP signaling group on Communication Manager and the **SIP Local** configuration on Client Enablement Services administration application are same. The protocol should be using either TCP or TLS.
5. Verify that the **Authoritative Domain** field value on the change ip-network-region page on Communication Manager and the value mentioned in the **Domain** field for

the Telephony server in the Client Enablement Services administration application are same.

6. If you have connected the Client Enablement Services server using secure connection or TLS over SIP trunk to Communication Manager, ensure that the certificate from Client Enablement Services is installed on Communication Manager.

   For more details on installing a certificate on Communication Manager, see *Administering Avaya Aura® Communication Manager*.

Avaya one-X® Client Enablement Services server page error

When you try to access any page of the Client Enablement Services administration application except the Login page using the browser history, you might get the following error message:

```
Error encountered while initializing the page.
```

Proposed solution

Procedure

To clear the error message and access the page you want to, click on any tab or link on the Client Enablement Services administration application screen.

Therefore, as a best practice you should not use the browser history to access any page of the Client Enablement Services administration application except the Login page.

Appendix A: Avaya one-X® Client Enablement Services certificates

If you have configured the Client Enablement Services for a functionality, ensure that the system displays the required certificate alias in the table on the Presence server page. Following is a list of Client Enablement Services functionalities and required trust store certificates.

Functionality: Secure SIP connection with Session Manager and Communication Manager

Required certificates (aliases)	avayasip and avayaproductroot
When are these imported?	During Client Enablement Services installation.
When does the import fails?	The import should not fail. The required certificates are always imported regardless of user input.

Functionality: Presence

Required certificates (aliases)	System Manager CA certificate. Alias is the 24 hexadecimal digit fingerprint of the certificate. For example, a1f04ae913b089f2335e2ff9.
When are these imported?	During Client Enablement Services installation.
When does the import fails?	The import fails if during installation, • the user does not enter the IP address of the System Manager • enters incorrect IP address of the System Manager • enters incorrect System Manager enrollment password • if System Manager is not running during Client Enablement Services server installation • if you enter the details of a System Manager other than the one configured for Client Enablement Services server

	Note: If you import the certificate from another System Manager, which is not configured in the Client Enablement Services server, the Presence Services server page displays the 24 hexadecimal alias for the wrong System Manager CA certificate. To identify this, you have to verify the wrong smgr.host property in the `/opt/avaya/1xp/config.properties` file. It is mandatory that the Presence Services server and Client Enablement Services server use the same System Manager to import their System Manager CA certificate. During Client Enablement Services installation, the System Manager CA certificate is imported into the Client Enablement Services server trust store. Client Enablement Services enforces System Manager to generate and sign the personal certificate of Client Enablement Services. Avaya products such as the Presence Services server trust the Client Enablement Services certificate because the System Manager CA signs this personal certificate. If Client Enablement Services and Presence Services get their certificates from different System Managers, then this trust does not exist, and the two servers do not communicate.
Resolution	When the System Manager is running, perform the following actions: 1. Log in as root to run this script from the command line. 2. ssh into the Client Enablement Services server using the command **`cd /opt/avaya/1xp`** 3. Run the command **`./run_config_smgr_jython.pl <smgr_enrollment_password>`** If Client Enablement Services is configured with a different System Manager that is configured in the Presence Services server, configure the correct System Manager in the Presence Services screen in the Client Enablement Services server administration application. Then run the command **`./run_config_smgr_jython.pl <smgr_enrollment_password>`**. **Note:** Periodically, depending on the expiry date of certificates in System Manager, retrieve and install new certificates by running the **`./run_config_smgr_jython.pl <smgr_enrollment_password>`** command as administrator.

Functionality: WebLM (centralized on System Manager)

Required certificates (alias)	System Manager CA Cert (see the Presence functionality for details). **Note:** Ensure that the WebLM is on the same System Manager from which the Client Enablement Services server gets its certificate.

Functionality: WebLM (from local CDOM)

Required certificates (alias)	cdomweblm
When are these imported?	During Client Enablement Services installation.
When does the import fails?	The import should not fail. The required certificates is always imported regardless of user input.

Functionality: Administration of local IBM HTTP Server from Client Enablement Services server

Required certificates (alias)	localwebserveradmin
When are these imported?	During Client Enablement Services installation.
When does the import fails?	The import should not fail. The required certificates is always imported regardless of user input. **Note:** This certificate is used by the WebSphere to update the plug-in on the local IBM HTTP Server.

Functionality: Administration of DMZ IBM HTTP Server

Required certificates (alias)	dmzwebserveradmin
When are these imported?	During Client Enablement Services installation.
When does the import fails?	The import can fail if the DMZ HTTP Server is not running during the installation of Client Enablement Services server, or if the dmz.ihs.host property in `/opt/avaya/1xp/config.properties` is not correctly set to the inward facing IP address of the DMZ server. **Note:** This certificate is used by the WebSphere to update the plug-in on the DMZ IBM HTTP Server.

Resolution	Correct the dmz.ihs.host property if this is set incorrectly, and then while Client Enablement Services server and the DMZ HTTP Server are running, run the following command:
	`cd /opt/avaya/1xp`
	`./run_config_httpservers_jython.pl`

Functionality: Client Enablement Services server integration with a voice messaging server

Required certificates (alias)	Certificate of the voice messaging server. Alias can be the IP address of either the Modular Messaging, or the Messaging, or the Communication Manager Messaging message store. For example, 148.147.34.41.
When are these imported?	This certificate is imported during administration of the voice messaging server in the Client Enablement Services administration application, when the administrator clicks the **Retrieve SSL Certificate** button while setting up the messaging server.
When does the import fails?	The import fails when the administrator does not click the **Retrieve SSL Certificate** button in the Client Enablement Services administration application, or if the messaging server was down when the administrator clicked the **Retrieve SSL Certificate** button.
Resolution	To get the SSL certificate, perform the following: 1. In the Client Enablement Services server administration application, go to **Servers** > **Voice Messaging**. 2. In the Voice Messaging Servers page, in the **Handle** column, click the link of the messaging server. 3. In the View Voice Messaging Server page, click **Retrieve SSL Certificate**. If the certificate is successfully retrieved, the button label changes to **Remove SSL Certificate**.

Index